



Missouri Division of Workforce Development
DWD Issuance 13-2016

Updated: August 14, 2017; February 28, 2019; March 28, 2019
Effective: March 13, 2017



Subject: Confidentiality and Information Security Plan for the Workforce Development Statewide Electronic Case Management System

1. Purpose: This Issuance communicates the Division of Workforce Development's (DWD) updated Confidentiality and Information Security Plan, including protocols for breaches of data, to all appropriate data users and their supervisors. The attached Plan includes a required attestation form all must sign prior to becoming authorized users.

2. Background: The Missouri Department of Economic Development (DED) "Acceptable Computer Use Policy" (*Attachment 2*) governs the use of State systems and applies to all DED employees, including DWD employees, and **all DED system users**.

This update of DWD's "Workforce Development System Confidentiality and Information Security Plan" (*Attachment 1*) reflects new terminology as well as statutory, regulatory, and procedural revisions necessitated by the Workforce Innovation and Opportunity Act (WIOA).¹ Joint federal regulations implementing WIOA (*Attachment 3*) expand the allowable information exchanges and records matching between workforce and education agencies. Active federal guidance on the handling and protection of Personally Identifiable Information (PII) published since the previous Issuance is also included (*Attachment 4*).

3. Substance: DWD's updated "Workforce Development System Confidentiality and Information Security Plan" describes:

- Sources of confidential information and user authorization;
- Privacy obligations and training requirements for authorized users, as well as attestation requirements before authorization is given;
- Procedures for the storage and sharing of confidential information;
- Data breach reporting, assessment, and mitigation procedures;
- Proportional responses and corrective actions for internal breaches;
- Procedures for permissible disclosures to third parties; and
- Legal references affecting privacy, confidentiality, disclosure, and security.

Any corrective actions affecting employment described in this Plan specifically refer to actions taken by the State regarding State employees. Nevertheless, the decision to grant access or to suspend access, for any user on any system administered by the State, is reserved to the State.

4. Action: This Issuance is effective immediately. It remains applicable to any future Statewide Electronic Case Management System administered by the Division of Workforce Development.

¹ Pub. Law 113-128 [29 U.S.C. 3101 et seq.].

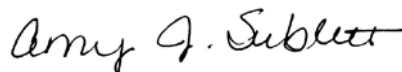
Distribute the “Workforce Development System Confidentiality and Information Security Plan” to all potential data users and supervisors among Local Workforce Development Boards (WDB), their staffs, subrecipients, and partner agencies. All recipients of this distribution must familiarize themselves with the Plan contents.

Any Local WDB that maintains its own local-level confidentiality plan must ensure that its plan is in concurrence with DWD’s “Workforce Development System Confidentiality and Information Security Plan.” Local WDBs are also responsible for ensuring their subrecipients’ data confidentiality plans are in concurrence with both the State and local plans.²

Local WDBs must make provisions in **Local Plans** and in **Memoranda of Understanding** to designate an individual as the local custodian of the Local Workforce Development Area Confidential Information Authorized Users List. That custodian will establish local procedures for list maintenance and synchronize updates to that list with the DWD Technical Support Unit (TSU).

5. Contact: Direct questions or comments regarding this Issuance to the DWD Technical Support Unit Manager at (573) 526-8258, or nico.gage@ded.mo.gov.
6. References: None.
7. Rescissions: This Issuance supersedes and replaces DWD Issuance 01-2008, Change 2, “Workforce Development System Confidentiality and Information Security Plan, Breach of Toolbox Data Confidentiality Update,” September 15, 2011.
8. Attachments: Attachment 1: “Workforce Development System Confidentiality and Information Security Plan”
Attachment 2: Missouri Department of Economic Development, “Acceptable Computer Use Policy,” July 7, 2017.
Attachment 3: 20 CFR Part 603 “Part 603—Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information” (as amended by the WIOA Final Rules).
Attachment 4: U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) No. 39-11, “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” June 28, 2012.

The Missouri Division of Workforce Development is an equal opportunity employer/program.
Auxiliary aids and services are available upon request to individuals with disabilities.
Missouri TTY Users can call (800) 735-2966 or dial 7-1-1.



Amy Sublett
Acting Director
Missouri Division of Workforce Development

² Uniform Guidance at 2 CFR 200.303(e), “Internal controls.”



Missouri Division of Workforce Development

Workforce Development System Confidentiality and Information Security Plan

Section:

- 1. PURPOSE**
- 2. DEFINITIONS**
- 3. SOURCES OF CONFIDENTIAL INFORMATION**
- 4. LEGAL REQUIREMENTS**
- 5. PROCEDURES**
 - 5.1 Authorized users
 - 5.2 Training of authorized users
 - 5.3 Access eligibility and registry process
 - 5.4 Acknowledgement of confidential information
 - 5.5 Medical- and disability-related information
 - 5.6 Storage of confidential information
 - 5.7 Sharing of confidential information
 - 5.8 Destroying confidential information
 - 5.9 Data breaches in general
 - 5.10 Breach of statewide electronic case-management system confidentiality
 - 5.11 Mitigation of a breach
- 6. INFORMED CONSENT AND PERMISSIVE DISCLOSURES**
- 7. LEGAL, REGULATORY, AND POLICY REFERENCES**
- 8. ACRONYMS USED IN THIS GUIDE**
- 9. FORMS**
 - Confidential User Attestation Form

The Missouri Division of Workforce Development is an equal opportunity employer/program.
Auxiliary aids and services are available upon request to individuals with disabilities.
Missouri TTY Users can call (800) 735-2966 or dial 7-1-1.

1. PURPOSE

The Workforce Innovation and Opportunity Act (WIOA)¹ (as well as other laws affecting Trade Act Assistance, education, and social services) directs the Missouri Workforce Development System. That system includes the Missouri State Workforce Development Board, the Division of Workforce Development (DWD), Local Workforce Development Boards (Local WDBs) and their subrecipients, and partner agencies. Among those partners, DWD collaborates most closely with the Missouri State Education System and the Division of Employment Security, which require additional safeguards peculiar to their databases. All these entities use confidential information daily.

This Plan is for Workforce Development System users of confidential information and their supervisors. It discusses defense against external attacks on information security and reducing breaches due to internal errors and misuse. This Plan also establishes a “proportional” response to accidental breaches. The best defense is having conscientious users committed to protecting the security of customers’ information.

The Workforce Development System must ensure the privacy of customers and safeguard their confidential information. Those actions serve customers by:

- protecting customers’ eligibility for workforce programs, services, and benefits;
- maintaining consumer confidence in the workforce development system by preserving privacy and minimizing the risk of identity theft² or fraud³; and
- shielding customers from discriminatory programmatic or hiring practices by keeping certain details about their barriers to employment in strict confidence.

This plan defines “confidential information.” It establishes procedures for preventing access by “unauthorized users.” Numerous federal, State, and local laws, regulations, and policies have confidentiality requirements. The assurances of contracts and agreements often compel compliance with some of these requirements. However, many fail to define the expected compliance. Therefore, this policy elaborates on several of those requirements.

The WIOA rules require confidentiality policies, such as this Plan, to protect Personally Identifiable Information (PII):

“Recipients and subrecipients of WIOA title I and Wagner-Peyser Act funds must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information, records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that the Department or the recipient or subrecipient considers to be sensitive, consistent with applicable Federal, State and local privacy and confidentiality laws.”⁴

A Local WDB’s Confidentiality and Information Security Plan must concur with *this* Plan. Local WDBs must ensure that subrecipients’ confidentiality policies concur with *both* plans.⁵

¹ Pub. Law 113-128 [29 U.S.C. 3101 et seq.].

² “Identity theft” involves the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law. (Pub. Law 105-318, “Identity Theft Assumption and Deterrence Act” [18 U.S.C. 1028]).

³ As used in this Plan, “fraud” covers a wide range of financial crimes, including credit-card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government-documents or benefits fraud, loan fraud, and health-care fraud.

⁴ 20 CFR 683.220(a).

⁵ Uniform Guidance at 2 CFR 200.303(e), “Internal controls.”

2. DEFINITIONS

2.1 Authorized users:

Workforce Development staff, Employment Security staff, and applicable Education system staff are among authorized users, as are other entities or persons having routine access to workforce, wage record, or education system confidential information or data. Supervisors identify authorized users on the Confidential Information Authorized User List. No organization, entity, or person currently under suspension or debarment by any State or federal agency may have access to secure data systems.⁶

2.2 Breach:

A *breach* is an unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A *breach of security* is “unauthorized access to, and unauthorized acquisition of, personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.”⁷ Four causes of breaches are:

- Malware and hacking — Breaches caused by intentional intrusions into computer systems by unauthorized outsiders with malicious or criminal intent.
- Physical breaches — The theft or loss of unencrypted data (or access codes or passwords) stored on laptops, desktop computers, hard drives, USB drives, data tapes, or paper documents.
- Errors — Breaches that result from anything authorized users unintentionally do, or leave undone, that exposes personal information to unauthorized individuals.
- Misuse — Breaches resulting from “trusted,” authorized users intentionally using privileges with willful disregard or in unauthorized ways for personal purposes.

Unauthorized discussion of a breach with co-workers or others is *also* a breach. Gossip can seriously obstruct internal reviews or external criminal investigations.

2.3 Confidential information (see also “Personally Identifiable Information”):

Any PII that alone, or in combination, is linked or linkable to a specific person or employer that would allow identification of that individual or employer. Unless otherwise required by law to be disclosed, it may include, but is *not limited to*:

- Name
- Social Security Number (SSN)
- Passport number, driver’s license number, or any unique government-issued ID number
- Ethnicity
- Age
- Date of birth
- Gender
- Addresses
- Email addresses
- Telephone numbers
- Physical description
- Family and household composition
- Domestic violence
- Education
- Medical or disability history
- Employment history

⁶ Executive Order (EO) 12549, Feb. 18, 1986; 29 CFR 94.630; and 2 CFR Part 180.

⁷ RSMo 407.1500.1(1).

- Wages or wage histories⁸
- Benefits and reimbursed expenses
- Dates and locations of services and training received
- Federal Employer Identification Number (FEIN)
- North American Industrial Classification System (NAICS) and other industry codes
- Unemployment Insurance (UI) claims, payments, or benefits information
- UI account information or status
- Financial matters or bank account information
- Credit or debit card numbers or account information
- Information about employees
- Employer history
- Salaries

“Confidential” includes statements made by, or attributed to, the individual or any employer.

2.4 Disability-related information:

Any information, whether oral or written, in any form or medium, relating to a physical or mental impairment that substantially limits one or more major life activities.

2.5 Disclosure:

To disclose, release, transfer, disseminate, or otherwise communicate all or any part of confidential information, records, or data verbally, in writing, electronically, or by any other means to any person or entity.

2.6 Incident: ⁹

An occurrence that:

- actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

2.7 Information security: ¹⁰

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Information security provides:

- integrity—guarding against improper information modifications or destruction, and ensuring information is authentic and irrefutable;
- confidentiality—preserving authorized restrictions on access and disclosure to protect personal privacy and proprietary information; and
- availability—ensuring timely and reliable access to, and use of, information.

⁸ Missouri State law imposes criminal penalties for unauthorized public disclosures of Division of Employment Security wage records that reveal an individual or employer’s identity (RSMo 288.250). The first offense of this statute is a Class A misdemeanor subject to up to \$10,000 in fines and/or one year in jail. A subsequent continuing offense is a Class E felony, subject to up to \$10,000 in fines and/or four years’ imprisonment.

⁹ Federal definition at 44 U.S.C. 3552(b)(2), Federal Information Security Modernization Act (FISMA) of 2014, as amended.

¹⁰ Federal definition at 44 U.S.C. 3552(b)(3), Federal Information Security Modernization Act (FISMA) of 2014, as amended; *see also* National Institute of Standards and Technology, FIPS Pub 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.

2.8 Medical and disability information:

Any information, oral or written, in any form or medium, relating to the past, present, or future mental or physical condition of an individual or to the provision of medical services. Although the *existence* of a disability or medical condition is collected as a customer record data element, specific details must be maintained in a separate secure location.¹¹ Rules changes from the U.S. Department of Labor (DOL) Civil Rights Center emphasize the confidentiality distinction between knowledge *of* a condition or disability and access to *details* of that condition or disability, on a “need-to-know” basis:

*“...the range of persons who may be permitted to have **access to files** containing medical and disability-related information about a particular individual is **narrower** than the range of persons who may be **permitted to know generally** that an individual has a disability. These changes make the regulations consistent with DOL’s regulations implementing § 504 of the Rehabilitation Act, and with the EEOC’s regulations implementing Title I of the ADA. The change is also intended to provide recipients with information necessary to enable them to develop protocols that are consistent with these requirements.”*¹²

2.9 Partners or partner agencies:

Any *State agency* that is part of the Missouri Job Center system [besides the Department of Economic Development (DED)/Division of Workforce Development (DWD)], including:

- Office of Administration (OA)
 - OA Information Technology Support Division (ITSD)
- Department of Labor and Industrial Relations (DOLIR)
 - DOLIR Division of Employment Security (DES)
- Department of Social Services (DSS)
 - DSS Family Support Division (FSD)
 - Rehabilitation Services for the Blind (RSB)
- Department of Corrections (DOC)
- Department of Elementary and Secondary Education (DESE)
 - DESE Division of Learning Services, Office of Adult Learning and Rehabilitation Services, Vocational Rehabilitation (VR)
 - DESE Division of Learning Services, Office of Adult Learning and Rehabilitation Services, Missouri Adult Education and Literacy (AEL) Program
- Coordinating Board for Higher Education (CBHE)
- Department of Health and Senior Services (DHSS)

This includes State agencies acting under the delegated authority of the above-listed agencies. Local WDBs and their subrecipients are also partner agencies.

The term “one-stop partners” specifically refers to WIOA-designated entities¹³ that provide access to their programs and services through the comprehensive one-stop center, contribute to its operation and maintenance, and are parties to a Memorandum of Understanding with the other WIOA-designated partners.

¹¹ DWD Issuance 02-2017, “Statewide Case Note Policy,” August 11, 2017. [This State records-isolation policy is now also federal policy, per the new rule at 29 CFR 38.41(b)(3)].

¹² Preamble commentary for 29 CFR 38.41(b)(3), *Notice of Proposed Rulemaking*, 29 CFR Part 38, “Implementation of the Nondiscrimination and Equal Opportunity Provisions of the Workforce Innovation and Opportunity Act, 81 FR 4493-4571, January 26, 2016. Final Rules for Part 38 were published on December 2, 2016, and became effective on January 3, 2017.

¹³ WIOA sec. 121(b); [29 U.S.C. 3151(b)].

2.10 Personally Identifiable Information (PII) *(see also Confidential Information):*

Information in records, such as a name or identification number, used to distinguish or trace an individual's identity, directly or indirectly, through linkages with other information. PII includes not only *direct* identifiers, like name and SSN, but also *indirect* identifiers such as date-and-place of birth. PII includes any information that, alone or in combination, is linked or linkable to a specific person that would allow identification of that person. The federal Office of Management and Budget (OMB) Uniform Guidance¹⁴ notes that:

“Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be ‘Public PII’ and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.”

For example, a name selected randomly from a phone book is not confidential. That name, when also identified as a Job Center customer, *becomes* a confidential piece of information. The OMB Uniform Guidance establishes the general premise that **linkage** of certain pieces of PII is what determines the need for confidentiality:

*“Protected PII means an individual’s first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date-and-place of birth, mother’s maiden name, criminal, medical, and financial records, [and] educational transcripts. This does not include PII that is required by law to be disclosed.”*¹⁵

2.11 Sensitive information:

Any unclassified information whose loss, misuse, or unauthorized access to, or modification of, could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974.^{16, 17}

¹⁴ 2 CFR 200.79.

¹⁵ 2 CFR 200.82

¹⁶ The OMB Uniform Guidance, including some of the above definitions, is recapped in U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) No. 39-11, “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” June 28, 2012, which is included as *Attachment 4* to the accompanying Issuance.

¹⁷ The Privacy Act of 1974, as amended, principally deals with the contents and disclosure procedures for records kept by *federal* agencies, as well as individuals’ access to those records. However, some federal awards and grants require recipient’s assurances to abide by certain requirements or procedures in the Act.

3. SOURCES OF CONFIDENTIAL INFORMATION

3.1 Sources of confidential information in the workforce system include:

- 3.1.1 Customer individual record files (paper copy, statewide electronic case-management system [SECMS] case files, etc.) and eligibility documentation.¹⁸
- 3.1.2 DWD SECMS Reports (Employment and Training Reports, assessment records, performance outcomes, etc.).
- 3.1.3 Individual performance roster data.
- 3.1.4 Unemployment Insurance (UI) wage records.
- 3.1.5 Wage Record Interchange System (WRIS) data.
- 3.1.6 The Work Opportunity Tax Credit (WOTC) database.
- 3.1.7 U.S. Department of Labor Workforce Integrated Performance System (WIPS).¹⁹
- 3.1.8 National Reporting System (NRS).
- 3.1.9 State Education System records (*see also Section 4.5*).

3.2 DWD oversees or operates various federal and State programs that collect confidential information on customers. The Local WDBs also contract with service providers that use confidential information in their operations. A customer's **confidential information may be shared** among various *authorized* users at partner agencies that coordinate services through the Workforce Development System, *provided* it is for the *sole intention* of fulfilling an employee's job duties to deliver authorized services to the customer or program participant.

3.3 The complainant's name and other particulars, records, or interviews associated with any **Equal Opportunity complaint** under WIOA Section 188 must be kept confidential.²⁰ This includes *any* information that could identify a particular individual as having filed a complaint.

3.4 The complainant's name and other particulars, records, or interviews associated with any **Wagner-Peyser Employment Service complaint** are confidential,²¹ including *any* information that could lead to identification of a particular individual as having filed a complaint.

3.5 Consistent with the above confidentiality, it is State policy that the complainant's name and other particulars, records, or interviews associated with any **WIOA programmatic complaint** under WIOA sec. 181(c) Grievance Procedures²² are also confidential, including *any* information that could lead to identification of a particular individual as having filed a complaint.

¹⁸ This includes all eligibility documentation as required by DWD Issuance 08-2018: "WIOA Adult and Dislocated Worker Programs Eligibility and Documentation Technical Assistance Guidance," March 19, 2019, and by DWD Issuance 09-2018: "Workforce Innovation and Opportunity Act Youth Program Eligibility and Documentation Technical Assistance Guidance," March 19, 2019.

¹⁹ Unauthorized use or misuse of WIPS may be subject to federal fines or imprisonment (18 U.S.C. 1030).

²⁰ 29 CFR 38.41(c).

²¹ 20 CFR 658.411(a)(3).

²² Implemented at 20 CFR 683.600.

4. LEGAL REQUIREMENTS

- 4.1 Numerous State and federal legal provisions cover various programs and services offered through the State workforce development system. (Section 7 lists some prominent legal provisions. This list is *not exhaustive*. Various other civil and criminal provisions surround confidential information and/or identity theft and may apply to this Plan.)
- 4.2 The Annual Agreement contract between DWD and each Local Workforce Development Area (LWDA), through the Chief Elected Official (CEO) or the CEO's Local Fiscal Agent (LFA), specifies confidentiality requirements in its Assurances. Local Areas *and* their subrecipients must comply with the confidentiality requirements of WIOA Sec. 116(i)(3)²³ and with the internal controls protection requirements for non-Federal recipients in the Uniform Guidance at 2 CFR 200.303. Conformity with this section is requisite to continuity of funding.
- 4.3 Missouri State Law²⁴ **requires notification** of an individual in the event of an uncontained breach of certain data elements of that individual's personal information. The law requires additional procedures if a breach involves a large number of individual records. Besides commercial databases, this statute specifically applies to government, governmental subdivisions, governmental agencies, and governmental instrumentalities. (*See Section 5.9.5.1 for more discussion.*) Therefore, all data breaches **must** be reported.
- 4.4 DED policy²⁵ obligates DWD employees to confidentiality and information security:
- An employee is prohibited from using information learned in the performance of job duties for personal benefit, including favoritism, professional advancement, or monetary gain;
 - An employee is responsible for safeguarding confidential/sensitive information;
 - An employee may not disclose confidential information obtained in the performance of duties to anyone in the Department who does not have a need-to-know or authority to receive such information;
 - An employee shall not seek information for which the employee does not have a need-to-know or the authority to receive;
 - An employee shall not disclose confidential information to individual(s) outside of Departmental personnel except as required by law; and
 - An employee must inform his/her supervisor or manager if he/she receives information to process on a relative or friend. The supervisor or manager will reassign the request to another staff member.

DWD expects all authorized users to adhere to these same rules.

- 4.5 The federal Family Educational Rights and Privacy Act (FERPA)²⁶ mandates certain confidentiality protocols involving student records. Compliance with FERPA is incorporated by reference into several Missouri education and privacy statutes.²⁷

²³ This section references compliance with Section 444 of the General Education Act (20 U.S.C. 1232g), also known as The Family Educational Rights and Privacy Act (FERPA). It provides for confidentiality of student records and open access to the records of minor children by their parents or guardians.

²⁴ RSMo 407.1500, "Definitions—notice to consumer for breach of security, procedure—attorney general may bring action for damages."

²⁵ DED "Personal Accountability and Conduct" policy, September 21, 2016.

²⁶ Section 444 of the General Education Provisions Act, Pub. Law 93-380, as amended [20 U.S.C. 1232g].

²⁷ RSMo 161.096, 161.825, and 210.145.

5. PROCEDURES

5.1 Authorized users:

- 5.1.1 DWD Central Office staff that have access to confidential information include the Director, Assistant Directors, Program Administrators, Central Office Managers, and their designated staffs. Others with access may include staff from ITSD, Performance and Planning, Quality Assurance, JobStat, Training, Technical Support, Financial, and other staff designated by their supervisors, and federal program staff.
- 5.1.2 Local staff with access to confidential information includes Local WDB members and staff and subrecipients, Functional Leaders, partner agency staff, and local DWD staff. It is the responsibility of the various organizations' supervisors to determine which individuals should be designated as authorized users.

5.2 Training of authorized users:

- 5.2.1 Confidentiality and Information Security training will be determined and administered by the DWD Technical Support Unit (TSU). This training will familiarize all users with privacy issues. It will provide guidelines for the use of confidential data maintained by DWD, Local WDBs and their subrecipients, and partner agencies. All users will be required to receive this training and sign the Confidential Information User Attestation Form (UAF) (*see Section 9, "Forms"*) prior to receiving access to confidential information. This includes access to certain websites or systems (such as the SECMS, UI Reporting, DRVS, etc.) that contain confidential information.

TSU may require training and signing of the UAF to be repeated in cases of:

- expired passwords;
 - lengthy periods between access or use;
 - a change in the user's employer of record;
 - retraining to correct user errors;
 - new legal, regulatory, or policy requirements; or
 - system updates or technical alterations.
- 5.2.2 System Access Request Forms (DWD-4) for partner users must be counter-signed and dated by the immediate supervisor and the DWD TSU individual assigned to maintain the Confidential Information Authorized User List.
- 5.2.3 Training must advise a prospective authorized user of the following State information-security concepts:²⁸
- Never share passwords with anyone, including help-desk staff.
 - The password confirms identity. Persons are responsible for anything performed under the assigned username and password combination. Access may be granted to supervisors and co-workers to the email application information without sharing the password.
 - Create strong passwords by including special characters and using both upper- and lower-case letters.
 - Do not write user ID or passwords down and leave them unattended.

²⁸ Missouri Cyber Security State Employee Computer Security Tips(https://cybersecurity.mo.gov/employee_tips/)

- Leaving post-it notes or other loose paper containing passwords near computers jeopardizes access to sensitive information.
- Always encrypt and password-protect sensitive information.
 - Social Security numbers, credit-card numbers, and healthcare information are protected by State and federal law. By default, email offers no information security. Any sensitive information, whether residing on a network, a share drive, or other storage device, must be encrypted.
- Always lock computers when leaving the workspace.
 - Locking computers protects logged-in accounts, such as email and network shares, from unauthorized use.
- Always store CDs, USB drives or other removable devices containing sensitive information in locked drawers.
 - Physically securing workspace devices deters unauthorized access.
- Professional IT staff must properly erase any electronic device used to store State information *before* it is discarded or disposed of via property transfer or surplus.
 - Sensitive information is still accessible—even after files have been deleted and a storage device has been reformatted.
- Use the network drives provided to save all important files and documents.
 - These drives are routinely backed up to prevent data loss.
- Connect State-issued laptops to the State’s network every 30 days or less for security updates and patches.
 - Ensuring that assigned laptops are up-to-date with the latest security updates and patches prevents future problems.
- Do not install third-party software applications without IT approval.
 - Always check with professional IT staff prior to installing any third-party software. Shareware often carries strict licensing requirements. Software also may have compatibility or vulnerability issues.
- Never open email attachments if unsure about its file type or purpose.
 - Even if an attachment appears to be from a friend or coworker, think twice before opening.
- Email messages sent become the property of the recipient.
 - Emails to and from State government websites or addressees also may be publicly accessible under the provisions of the Missouri Sunshine Law (RSMo Chapter 610).
- Think before clicking on a link.
 - Don’t immediately trust links provided within email messages, PDFs, search engine results, or even trusted websites. If suspicious, do not click on the link.

5.3 Access eligibility and registry process:

- 5.3.1 DWD TSU will maintain the Confidential Information Authorized User List composed of the SECMS and other online data systems users.
- 5.3.2 Local WDB Directors and Functional Leaders will oversee this process for LWDAs and Missouri Job Centers (and subrecipients), ensuring that all partners properly maintain their user lists. (DWD TSU will oversee the local DWD staff.) This custodial role must be included in the local Memorandum of Understanding and the Local Plan. DWD may monitor for compliance.
- 5.3.3 Supervisors of authorized DWD staff users will be responsible for ensuring that staff have been trained and that they have signed their UAFs.

For partner agency staff, the Missouri Job Center Functional Leader will submit completed UAFs to the respective agency's personnel office.

- 5.3.4 When posting names to the Confidential Information Authorized User List, the supervisor also will designate the types of information the user will be accessing (i.e., UI data, SECMS, and Performance rosters).
- 5.3.5 DWD's TSU will provide access (including requests from Local WDBs) to authorized users.

5.4 Acknowledgement of confidential information:

- 5.4.1 Jobseeker customers creating new accounts on *jobs.mo.gov* are informed about information they submit:

"You are accessing a trusted, secure government website. The State of Missouri does not share your personal information with other entities. For more information about the State of Missouri Privacy Policy, go to www.mo.gov/privacy-policy."

Customers registering in-person with Job Center staff also must be reminded of this statement.

- 5.4.2 Paper copies of confidential information should be marked, "Confidential."
- 5.4.3 Email and faxes are not secure transmissions for confidential information and have the potential of being viewed by unintended recipients. Before sending documents, verify the accuracy of email addresses and fax numbers. When faxing, call the recipient to ensure an authorized user will be receiving the fax. If an email or fax with confidential information is sent or received in error, notify the sender/receiver immediately with instructions for safeguarding the information.
- 5.4.4 Emails and faxes must not contain a customer's full Social Security Number (SSN). Rather, the customer's full name, with middle initial, followed by the last four digits of their SSN, the customer's programmatic identification code, or the SECMS Applicant ID (APPID) number, if applicable, will be used to protect their identity when providing communication documents.
- 5.4.5 Faxes and emails containing confidential information must include the statement below in the email or on the fax cover sheet. The fax form [DWD-ADM-2 (2015-03)] https://jobs.mo.gov/sites/jobs/files/fax_transmittal_rev03-2015_dwd-adm-2.pdf includes this language:

"CONFIDENTIALITY STATEMENT: This message and any attachments are intended only for those to whom it is addressed and may contain information which is privileged, confidential, and prohibited from disclosure or unauthorized use under applicable law. If you are not the intended recipient of this message, you are hereby notified that any use, dissemination, or copying of this email or the information contained in this message is strictly prohibited by the sender. If you have received this transmission in error, please return the material received to the sender and delete all copies from your system."

An email confidentiality tag line (message footer) containing the above advisory has been a required component of all DWD staff email correspondence signature blocks

and those of all partner staff SECMS users since 2008.²⁹ **This requirement remains in force.** This appropriately covers any intentional or unintentional inclusion of confidential client data. All SECMS users must use a confidentiality tag line similar to the one above. Users can copy and paste the text into their personal signature block in their email application. (For Microsoft Outlook users, this is usually accessed through **Tools>Options>Mail Format>Signatures.**)

- 5.4.6 *Receipt of unsolicited* confidential information or PII submitted via fax or email from customers to the State email-system users is *not* a breach of confidentiality or this Plan. The Missouri State Government Privacy Policy³⁰ provides legal notice for the entire “.mo.gov” domain that any emails to the State are not necessarily secure or confidential. When unsolicited PII is received electronically from a customer, it is advisable to send a follow-up reply (after *removing* the PII text in the original message) cautioning that customer to supply only information needed to answer a question or process a request. Once unsolicited confidential information or PII is received, however, its custody must be managed in a manner consistent with this Plan.

5.5 Medical- and disability-related information:

- 5.5.1 As per Section 5.6.2, keep medical- and disability-related information in a separate, secure location, physically removed from the main files for participants or employees. The Local WDB, partner agency staff, and DWD will take measures, with the support of ITSD, to ensure all access to medical- and disability-related information is treated every bit as “confidential” as other information identified in Sections 2.3 and 3. Electronic files must be password-protected and physical files must be kept in a secure, locked location.
- 5.5.2 The use or disclosure of medical- and disability-related information is limited to specific, lawful purposes.
- 5.5.3 Direct all inquiries or comments about secure medical and disability records to Danielle Smith, State Equal Opportunity Officer, at (573) 751-2428 or email danielle.smith@ded.mo.gov

5.6 Storage of confidential information:

- 5.6.1 Store confidential information that is in paper or portable media format in a secure location to prevent unauthorized access. “Secure location” means a locked drawer, file safe, cabinet, or room physically accessible only by a known list of authorized users.
- 5.6.2 Customer medical- and disability-related information must be stored in a separate, secure location. The location of the medical- and disability-related information must be noted in the customer’s main file.³¹ (*See also Section 5.5.*)
- 5.6.3 Confidential information stored electronically must be protected by security programs to prevent unauthorized users from accessing this information.

²⁹ DWD Issuance: 01-2008, “Division of Workforce Development Confidentiality and Information Security Plan,” September 1, 2008, and subsequent Change 1 (February 1, 2011) and Change 2 (September 15, 2011). ³⁰ <http://www.mo.gov/privacy-policy/>.

³¹ For detailed policy on proper service or case note procedures, see DWD Issuance 02-2017, “Statewide Case Note Policy,” August 11, 2017.

- 5.6.4 Authorized users must not leave confidential information exposed. Computers and screens should be “locked” (i.e., CTRL + ALT + DELETE) before leaving the work area. Authorized users also must avoid situations where unauthorized persons, such as other customers, can read records information displayed on the user’s screen.
- 5.6.5 Any portable-media electronic record containing confidential information (i.e., diskettes, disk drives, flash drives, CD-ROMs, tapes, etc.) must be properly secured (i.e., locked in a drawer or cabinet) to prevent unauthorized access.
- 5.6.6 When a staffing change occurs, it is the responsibility of the supervisor to ensure that all confidential information is returned and to terminate the departing user’s access, as appropriate. This includes, but is not limited to, submitting an Access Request (Form DWD-4) to DWD TSU within two weeks prior to the employment action taking effect, or as soon as possible, if not given notice.
- 5.6.7 *Social Security Numbers (SSNs)* — Whenever possible, use unique identifiers (such as Applicant IDs [APPIDs]) for participant tracking instead of SSNs after the SSN is entered for required federal performance tracking. If SSNs must be used for participant tracking, they must be stored or displayed in a way that is not linked to a particular individual, such as using a truncated (last-four-digits) SSN.

5.7 Sharing of confidential information:

- 5.7.1 Sharing confidential information is a necessity to operate the programs mentioned in Section 2 of this Plan. Any user of confidential information must be authorized. Authorized disclosures are of two types, permissive and required. Permissive disclosures involve a signed request from the subject of the information or a signed release directing that specific information be conveyed to a specific third party for a specific use. Required disclosures are releases of information mandated by law or regulation that do not require the informed consent of the subject of the information.
- 5.7.2 When transmitting paper copies of confidential information, they should be placed in folders or envelopes marked “Confidential.” These should be placed in a secure location when not in use.
- 5.7.3 When confidential information is subpoenaed as part of a civil or criminal case or investigation, DWD Administration will handle all such requests, and **no information is to be released at the local level without prior authorization from DWD.** Procedure must be followed according to 20 CFR Part 603.7. This Plan and Policy incorporates, by reference, 20 CFR Part 603 (*and any subsequent changes to that part; see Attachment 3 to the accompanying Issuance*).³² (*See also Section 6, “Informed Consent and Permissive Disclosures.”*). Besides the requirements of federal regulation, an interagency agreement between DES and DWD mandates these procedures. All authorized users must adhere to these requirements.
- 5.7.4 The 20 CFR Part 603 regulations permit disclosure of confidential Unemployment Compensation (UC) information to agents and contractors of public officials. State UC agencies may disclose confidential UC information to the agent or contractor of a public official so long as the public official has a written, enforceable agreement with

³² “Part 603—Federal-State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information.” The WIOA Final Rules amended sections 603.2, 603.5, and 603.6.

the State UC agency to obtain the data.³³ The public official must:

- agree to be responsible for any failure by the agent or contractor to comply with the safeguards and security requirements of 20 CFR 603.9 and 603.10(a);
- affirm that the confidential UC information will be used for a permissible purpose; and
- affirm that the requirements for all agreements in 20 CFR 603.10(b) are met.

In this context, an “agent” is a person or an entity acting instead of, and on the behalf of, a principal. A contractor is a person or entity with whom a public official enters into an agreement to provide services, usually, in this context, for data analysis. [“Public official” in this context is not the same as used in the subpoena provisions of 20 CFR 603.7, discussed previously in Section 5.6.3, or as used regarding an elected official acting as an agent, as discussed later in section 6.1.2.2.]

5.7.5 A record must be kept of all disclosures of PII to the customer, or to the customer’s agent, or to authorized third parties not involved with the day-to-day use of a customer’s PII. (That is, authorized everyday PII use by employees of the agency owning the database or its partner agencies does not need to be recorded.) Likewise, a record must be kept of all requests received for a customer’s PII, whether the request was fulfilled or not. These request and disclosure records must be retained for a period of at least five years, or the life of the PII record, whichever is longer.³⁴

5.7.6 *Encryption* — All grantees must comply with all of the following DOL Employment and Training Administration (ETA) policies:³⁵

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module.
- Grantees must not email unencrypted sensitive PII to any entity, including ETA or contractors.
- Accessing, processing, and storing of ETA-grant PII data on personally owned equipment at off-site locations (e.g., employee’s home, and non-grantee-managed IT services, such as private email servers) is strictly prohibited unless approved by ETA.
- Data may be downloaded to, or maintained on, mobile or portable devices only if encrypted using NIST-validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

³³ U.S. Department of Labor, Training and Employment Administration, Training and Employment Guidance Letter 7-16, “Data Matching to Facilitate WIOA Performance Reporting,” Attachment 1, “Joint Guidance with the Department of Education for Matching PII From Educational Records and Personal Information from Vocational Rehabilitation Records with Unemployment Compensation Wage Records,” August 23, 2016.

³⁴ This procedure complies with the Privacy Act of 1974 at 5 U.S.C. 552a(c).

³⁵ U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) No. 39-11, “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” June 28, 2012, which is included as *Attachment 4* to the accompanying Issuance

5.8 Destroying confidential information:

- 5.8.1 When paper or disposable media copies of confidential information are no longer needed, they should be disposed of according to applicable State and federal record-retention guidelines, and using appropriate methods (i.e., shredding on site, placing in a locked receptacle for shredding later, and otherwise ensuring they are not accessible to others) to maintain confidentiality.
- 5.8.2 Per Missouri statute³⁶ and policy,³⁷ electronic documents and emails on State email servers are archived and cannot be destroyed. Nevertheless, deletions can be made from a user's sent or received folders to prevent (further) dissemination of breached information. Because the server has captured a master image already, the statutory requirement is fulfilled. The State transparency statute also specifically bows to RSMo 610.21 in the Missouri Sunshine Law, which excludes 23 classes of records (including PII, as used in the workforce system) from public disclosure.

5.9 Data breaches in general:

- 5.9.1 The term “data breach” generally refers to the unauthorized or unintentional exposure, disclosure, or loss of sensitive information. A data breach can leave individuals vulnerable to fraudulent activity, (such as identity theft), discrimination (through breach of medical or disability information), or outright theft (breach of accountholder information).

Any disclosure of confidential information, whether unintentional (negligent or accidental) or intentional, to *unauthorized individuals* is considered a “**breach**.” Unauthorized **modifications** or **deletions** of information, or other violations of procedures listed in this Plan, are also “breaches.”

Information *regarding* a confidential security breach is *also* confidential information, and it must not be shared freely. Do not discuss the reporting of, assessment of, or response to a breach with anyone other than your immediate supervisor. Such actions may result in corrective, disciplinary, or legal actions.

As stated in Section 1, the goals of this plan are to safeguard customers and to secure their information. The purpose of this plan is not to perfect a punitive system for breaches. It is to manage information and case-management systems better by minimizing accidents and negligence.

- 5.9.2 **Incident response** — The phases of dealing with an incident are, generally: **reporting** the breach, initial **assessment** (risk analysis), **notification** (if necessary), **remediation**, and incident **review**.

All breaches, whether internal or external, must be **reported** to a supervisor, either by the “breacher” or by the first employee to discover the breach. Failure to report, or attempting a correction without first discussing with a supervisor, is as serious as a breach itself. *(If the breach involves up-line management, you may report directly to the DWD*

³⁶ RSMo 37.070, “Transparency policy—public availability of data—broad interpretation of sunshine law requests—breach of the public trust, when.

³⁷ Missouri Department of Economic Development, “Acceptable Computer Use Policy,” July 7, 2017 (*see Attachment 2 to the accompanying Issuance*).

Assistant Director for Administration. See Section 5.10.8.) Do not let personal embarrassment or fear of disciplinary action jeopardize our accountability to workforce customers. Do not self-correct a breach before a supervisor has assessed the situation and approved the action. It is equally incumbent on supervisors not to make breach reporting an uncomfortable or threatening experience. Supervisors (and Functional Leaders, where they serve as supervisors for non-State staff) must report all breaches of confidentiality to their superiors and to DWD TSU. **Reporting an incident is *not* “discretionary.”**

Do not assume that every incident actually *is* a breach of PII; it may not be. Validating that fact is part of assessment.³⁸ Nevertheless, a *suspected* breach should be reported.

Any sub-state local monitor, state-level DWD Quality Assurance monitor, or the DWD Technical Support Unit also may initiate a breach-incident report.

- 5.9.3 If the breach involves information from DWD or a partner agency (*see Section 2.9*), the user who discovered or detected the breach must notify the supervisor immediately. If the supervisor is, or is expected to be, absent, the supervisor’s superior should be notified of the breach. Otherwise, it is the supervisor’s responsibility to notify the agency’s appropriate up-line management.
- 5.9.4 If a breach occurs within DWD, the DWD Assistant Director for Administration (or assigned designee) will be responsible for notifying the partner agency owning the source information compromised.

If the breach occurs within a partner agency, the Director from that partner agency is responsible for notifying the partner agency that is the owner of the information compromised. (i.e., DWD or another agency listed in Section 2.9).

- 5.9.5 If a breach occurs, the agency owning or otherwise responsible for the database will be responsible for assessing whether the breach is significant enough to require advising the customer. If so, that agency will notify the individual or company about the breach (and arrange for mitigation services, if necessary).

If the notifying agency is a subrecipient acting under the authority of DWD, the DWD Assistant Director for Administration (or assigned designee) will be involved in the customer-notification process.

- 5.9.5.1. *Customer’s right to know* — As of the date of this Issuance, there is no general, overarching, *federal* data-breach law or regulation. There is no discussion of breach notification in either the DOL rules on UI-recipient data confidentiality³⁹ or in the U.S. Department of Education (ED) rules about student record-data confidentiality.⁴⁰

Nevertheless, **Missouri State law**⁴¹ *does* require DWD (and its subrecipients, as well as partner agencies), to notify the affected consumer (Missouri resident) of a breach of personal-information security *if* that breach includes,

³⁸ U.S. Department of Education “Data Breach Response Checklist,” PTAC-CL, September 2012.

³⁹ 20 CFR Part 603.

⁴⁰ 34 CFR Part 99.

⁴¹ RSMo 407.1500.

in an unredacted or unencrypted form, that individual's **first name (or first initial) and last name combined with *one or more* of the following data elements:**

- Social Security Number;
- Driver's license number or other unique identification number created or collected by a government body;
- Financial account number, credit card number, or debit card number in combination and access code or password;
- Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit account access;
- Medical information; or
- Health-insurance information.

If the agency's investigation of the breach determines, according to statutory guidelines, that the breach does *not* pose a risk of identity theft or fraud to the customer, notification may be determined to be unnecessary. However, that conclusion must be *documented in writing* and kept on file for a period of five years.

When customer notification *is* required, the process and the required contents and format of that notice are prescribed by statute. **Therefore, unauthorized persons *must not* contact the customer directly.** If a breach involves a large number (>1,000) of individual notifications, State law requires additional notifications to the Missouri Attorney General and certain consumer-reporting agencies.

5.10 Breach of statewide electronic case-management data confidentiality:

The following procedures address **internal breaches** of confidentiality due to system misuse or human error. In the event of an apparent or suspected **external** attack (a criminal intrusion) into the electronic case-management system, DWD TSU must be notified **within the hour** of first discovery. That notification should include preliminary details of how data **confidentiality, integrity, or availability** have been compromised (*see Section 2.7*) and whether the potential impacts in each of those three areas are **low, moderate, or high**.⁴²

- 5.10.1 The Department of Economic Development "Acceptable Computer Use Policy" (*Attachment 2 to the accompanying Issuance*) governs the use of State systems and applies to all DED employees and **all DED system users**. A supervisor's waiver, statement, or conduct **cannot** modify this policy.
- 5.10.2 Each DED system user is responsible for all computer/Internet use associated with his or her assigned user ID. It is prohibited for a DED system user to use another person's user ID and confidential password. DED system users **must not** give their user ID in combination with their password to any other individual, and must guard against unauthorized access to their assigned equipment. There may be some systems where there is an assigned group user ID, but passwords will be individualized.

⁴² That is, whether the damage is easily repairable, or requires immediate or emergency attention, or is irreparable and puts the agency at risk. (*See 5.10.3.4.*)

- 5.10.3 Although this policy refers to case-management system data, it also applies to any physical copies or representations of that data.

When notified by the user who caused a breach (or the first employee to detect the breach), the supervisor will perform a preliminary **assessment** of the breach **before** any mitigating, remedial, corrective, or disciplinary actions are taken. Time must be taken to determine the scope of a breach and to secure the system. *Treat the assessment itself as confidential information.*

The assessment, or risk analysis, should determine the **type** of breach, the **cause** of the breach, the **magnitude** of the breach, and recommend the first **proportional response** to the breach. **The supervisor's assessment and recommendation for corrective actions are subject to review and approval by DWD.**

5.10.3.1 This preliminary assessment should characterize the **nature** of the breach as:

- An *electronic* security breach (unauthorized storage, transmission, deletion, or alteration of files or records.); *or*
- A *physical* security breach (involving hard copies of data files or records, physical correspondence, or physical access to a secure storage, the workspace, or the premises in general).

Basic information concerning the breach should be recorded, including:

- The **person** causing (or the person detecting) the breach.
- The assigned **user ID and employer of record** for that person
- The **date** and estimated **time** of the breach, or its detection.
- The center, office, or other **location** where the breach occurred.
- In a case of compromised electronic communications or records, the **platform** involved (e.g., email, case-management system, website, etc.). Give the **physical location** in cases of breaches of physical security.
- Is the system or location currently **secure**, or is it still **vulnerable**? (Has system access been compromised, or has a lock been broken, etc.?)
- What general **type of information** is compromised (e.g., “name, DOB, and SSN,” “APPID and SSN,” “medical/disability,” etc.), and **how many records** are involved?
- Specify whether the unauthorized breach was a **deletion**, a **modification**, or an **exposure** of information.

5.10.3.2 Assess the **magnitude**⁴³ of the breach as:

1. **Other than Serious** — An inadvertent breach with minimal or no impact; situations where intra-agency, or interagency, mitigation of the breach can prevent widespread, or uncontrolled distribution of the compromised information). In short, any situation where the error can be contained and full confidentiality can be restored. “Other than serious” also may apply to cases where it is not possible to link the breached data with a specific individual or employer.
2. **Serious** — Examples include a risk to a customer’s identity, privacy, rights, benefits, or financial security; information that could lead to discrimination against the customer; information affecting multiple customers [e.g., lost lists]; agency, recipient, or subrecipient liability for fines or penalties; retaliation against a customer; or a breach of the material terms of an interagency agreement.
3. **Repeated Serious** — A violation (breach) of a **serious** nature that is materially similar to a prior serious breach in the past 12 months that required advanced corrective or disciplinary action, including access restrictions or suspensions.
4. **Willfully Repeated** — The user *knew* that a policy, regulation, or law prohibited his or her conduct but nevertheless disregarded, or acted with plain indifference to, that prohibition. **Moreover**, the breach is of such a nature that the recipient is bound to report it to the State, DOL, or another federal agency; it may involve civil monetary penalties, such as damages, fines, funding adjustments, restitution or protection for the customer; or if agency integrity is jeopardized.
5. **Pervasive Violation** — A case where an individual (and/or the *organization* that employs the individual), reflects a basic disregard for policies, regulations, and laws. That disregard is demonstrated by a pattern of serious and/or willful violations, continuing violations, or numerous violations. Pervasive violations must be multiple. Any organization that regards sanctions for violations as merely the “cost of doing business” must be considered to be a pervasive violator.⁴⁴ The State may initiate suspension of privileges, access, or funding for that partner, recipient, subrecipient, or contractor. The State also may commence debarment procedures to prohibit that organization from competing for or contracting for certain governmental services.
6. **Criminal activity or intent** — Cases where the mining, passing, or use of confidential information for personal gain, retribution, or advantage—including, but not limited to, monetary gain and bribery—is involved. This includes any *solicitation* by the authorized user(s) to pass along such information for personal gain, retribution, or advantage. The felony

⁴³ This scale derives from DOL guidance for characterizing violations of federal labor laws. It was published as Final Guidance for 48 CFR Parts 22 and 52 in the *Federal Register* on August 25, 2016 (81FR58653–58758).

⁴⁴ DOL Final Guidance at Section III(A)(4) “Pervasive violations,” 81FR58732.

offense of “acceding to corruption”⁴⁵ applies if a public servant knowingly solicits, accepts, or agrees to accept any benefit (direct or indirect) in return for his or her action (or withheld action) as a public servant. It includes violation of a known legal duty as a public servant. The “misuse of official information” is a misdemeanor under Missouri law.⁴⁶ “Misuse” refers to using insider confidential information about a customer for private gain. DWD will direct criminal activity cases to the attention of the appropriate authorities. Immediately report any evidence, or significant suspicion, of criminal activity by an authorized user to the DWD Assistant Director for Administration. This policy (Section 5.10.8) and federal law (41 U.S.C. 4712) mandate protection of whistleblowers from reprisals.

Regardless of the magnitude of the breach, the assessment must continue, to establish the *extent* of the breach and to determine mitigation requirements.

5.10.3.3 Preliminary assessment should then characterize the **cause** of the breach. Assess breaches on a case-by-case basis in light of the totality of the circumstances, including the severity of the breach, the user’s level and extent of access, and any mitigating factors. “No fault” breaches are rare, and responsibility should be assigned. In some cases, the organization employing the individual might be as culpable. Causes can be:

- **Negligence/Accident** (the breach of information or procedure was unintentional or unavoidable). Examples might include:
 - Failure to redact sensitive information, especially social security numbers, before sending or forwarding an email.
 - Accidentally emailing to the wrong person because of the mnemonic autocomplete feature in the “To...” window.
 - Attaching or inserting information in a reply and inadvertently clicking “Reply to All.”
 - Sending or replying to address groups or distribution lists that include unauthorized persons.
 - Hitting a preloaded addressee and emailing a copier/scanner document to an unintended recipient; leaving confidential information in public area printer/copier output trays.
 - Failure to place confidential files or portable storage devices in secure lockdown; failure to lock the secure location.
 - Online posting of sample text, PowerPoint examples, or desk aids that include actual customer data instead of mock data.
 - Online posting of sensitive information in unsecured website directories, even if that directory is invisible to a web browser.
 - Failure to check the content of attachments before forwarding.

⁴⁵ RSMo 576.020 “Public servant acceding to corruption—penalty.” This Class E felony carries penalties of up to \$10,000 in fines and/or up to four years’ imprisonment. Note that all state merit staff, city or county staff, Chief Elected Official appointees/designees, and Local WDB staff are public servants. See also DWD Issuance 23-2015, “Policy on Reports and Complaints about Criminal Fraud, Waste, Abuse, or Other Criminal Activity Related to Federal Awards,” June 14, 2016, and 2 CFR 200.113 “Mandatory disclosures.”

⁴⁶ RSMo 576.050, “Misuse of public information—penalty.” This Class A misdemeanor carries penalties of up to \$10,000 in fines and/or up to one year in jail.

- Failure to remove information about medical, disability, substance abuse, etc., from service notes to a separate secure location, per State policy and federal laws and regulations.⁴⁷
 - Access or performance was compromised when a user was hoaxed, allowing malware, phishing, spam, spyware, etc., into the system.
 - Compromised voicemail access or messages content.
 - Improper destruction of confidential documents (not shredding or placing in secure holding for shredding; i.e., placed in unsecured trash).
- **Willful disregard** for policies or procedures for reasons of apathy, sloth, or expediency. “Willful,” in a legal sense, means, “intentional,” as distinguished from “accidental” or “involuntary.” (An error based upon a mistaken understanding of proper procedure, done in good faith, would be *negligent*, not *willful*.) For this plan, “willful” means being fully aware of proper policies or regulations—and acting otherwise. Examples include:
 - Repeated specific errors, as per the above examples, in spite of specific correction or retraining.
 - Leaving a customer, or any other unauthorized person, unattended in a workspace or secure area; allowing them to sit in view of onscreen classified information or IDs/pass codes; failing to monitor access to the workspace or materials.
 - Posting/discussion of sensitive information on social-media sites.
 - Being aware of, but *ignoring*, protocols for securing or transmitting data, securing confidential files, or securing the desktop, workspace, or peripheral equipment (retrieving confidential output from copiers, printers, scanners, etc.)
 - An habitual unconcern with security procedures.
 - An unwillingness to change personal habits to accommodate security.
 - Bypassing security because of a deadline, a time-dependent request, or a similar excuse for “shortcutting” procedures, without supervisor approval.
 - **Suspicious activity** (unauthorized and potentially unlawful actions). Examples might include:
 - By adding “cc” or “bcc” recipients, distributing messages containing confidential information or PII to unknown or unauthorized addressees, or to personal email accounts.
 - Uploading data to unauthorized URLs or file-transfer portals.
 - Copying information to personal diskettes or flash drives; use of camera-phone to capture screen images or files.
 - Removing electronic or physical files, records, or printouts from the workplace.

Suspicious activity won’t be “self-reported.” Because it may lead to serious disciplinary or legal action, supervisors should be extremely prudent when

⁴⁷ DWD Issuance 02-2017, “Statewide Case Note Policy,” August 11, 2017; also 29 CFR 38.41(b)(3), “Collection and maintenance of equal opportunity data and other information.”

receiving reports of suspicious activity from one staff member regarding another. Impose a gag rule to avoid jeopardizing any investigation.

- 5.10.3.4 The supervisor's assessment should next quantify the **extent** (effect) of the breach. (This may be a preliminary guess. Subtle database alterations might only be apparent to an IT expert.) In general, though, estimate if the breach is:
1. easily **reparable** (low impact); or
 2. requires **emergency attention** (moderate impact); or
 3. is **irreparable** (high impact) and/or poses serious **liability** for the agency.

5.10.4 Answer the following questions to inform that assessment:

5.10.4.1 Is the confidential information or PII now available *outside* the universe of authorized workforce-development system users?

- For example, if this was a breach of procedure, does the confidential information remain in the hands of authorized users? That is, will redaction of messages or other materials seal this breach?

5.10.4.2 Does the compromised information pose a risk or threat of loss of rights, privileges, or benefits to the customer(s)?

5.10.4.3 Does the compromised information pose a risk or threat of identity theft, fraud, or cyberattack to the customer(s)?

5.10.4.4 Does the compromised information pose a risk or threat of information theft, fraud, or cyberattack to workforce records, systems, or websites?

5.10.4.5 Does this affect the performance or reliability of computer hardware or infrastructure seriously enough to involve OA-ITSD support services?

5.10.4.6 Does the compromised information pose a risk or threat to the records or systems of any partner agency or other subrecipient?

5.10.4.7 Does the compromised information or access pose a risk to the Intellectual Property (IP) rights of any of the State's software vendors?

5.10.4.8 Does the breach involve more than one individual's record? Provide an accurate-as-possible estimate of the number of records involved.

5.10.5 Apply a **proportional response** when assessing damage repair and corrective action for users involved in a breach. Several factors may weigh either in favor of **leniency** or in favor of **sterner measures**:

- Mitigating factors that weigh in favor of **leniency** may include:
 - Self-reporting of the breach.
 - Good-faith effort to comply with security procedures.
 - Remediation of the condition, behavior, or procedure that caused the breach, in an effort to prevent recurrences.
 - Only violation and/or a low number of previous significant violations. (However, "It's a first-time offense" does not negate the actual **effect** of a breach.)
 - A long, uninterrupted record of compliance.

- Recent legal or regulatory changes have not been delivered to the user as training or guidance.
- The user was acting on good faith and reasonable grounds; trusting a usually reliable co-worker or source that the action was within the bounds of proper procedure.
- Factors that weigh in favor of **more rigorous corrective measures** may include:
 - Intentionally disowning the breach or trying to cover it up.
 - Pervasive violations; another example in a pattern of basic disregard for proper security procedures.
 - Violations that are “willfully repeated” in magnitude *and* “willful” in causality, thereby indicating a disinterest in customer confidentiality. This is unacceptable for an authorized user, regardless of how minimal the damage may have been.
 - The gravity of the breach has serious financial consequences for the customer or serious operational, contractual, or legal consequences for the workforce system.
 - Any violation of a type for which a previous monitoring or independent audit issued an unresolved concern or a finding.
 - Repeat violations by an organization, or actions for which a federal or State agency already imposed suspensions or penalties.

5.10.6 *Evaluation* — Although there might be a situation where a “no-fault” ruling is justified, that decision is reserved to the DWD Assistant Director for Administration, not the supervisor.⁴⁸

The preceding risk-assessment process should have provided preliminary answers to the following questions:⁴⁹

- What is the nature of the data elements breached?
- What is the number of individuals (or companies) affected?
- What is the likelihood the information is accessible and usable?
- What is the likelihood the breach may lead to harm?
- What is the ability of the agency to mitigate the risk of harm?

The answers to these questions should influence scoring using the following incident-assessment tables.

⁴⁸ The DWD Assistant Director for Administration will function as the Senior Agency Official for Privacy (SAOP), using the federal vernacular of OMB Circular A-130, “Managing Information as a Strategic Resource,” July 2016.

⁴⁹ U.S. Department of Education, Departmental Directive OM:6-107, April 15, 2008, “External Breach Notification Policy and Plan.” *See also* National Institute of Standards and Technology, FIPS Pub 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.

5.10.6.1 Incident-assessment tables.

The following scoring-system tables should *guide* corrective or disciplinary actions that follow an assessment of an *internal* breach. This will provide a timesaving approach for supervisors to arrive at the proper proportional response to a breach. It allows them to hold, in that balance of judgment, the magnitude, cause, and effect of the breach. The supervisor should have latitude to weigh in additional mitigating or negative factors, as in Section 5.10.4 above, plus or minus five points in total. Any user who wishes to appeal the assessment and corrective action may do so within 30 calendar days of the decision. Appeals can be made to the DWD Assistant Director for Administration.

MAGNITUDE		CAUSE		EFFECT		
Other than Serious*	10	Negligence or Accident	5	Reparable†	10	25
Other than Serious	10	Willful	10	Reparable	10	30
Other than Serious	10	Suspicious	20	Reparable	10	40

* To be “Other than Serious,” the breach must not be as described in Section 5.9.5.1, *or* DWD must approve a written determination of “no risk” of identity theft or fraud.

† Given the definition of “Other than Serious,” only “Reparable” effects are possible.)

MAGNITUDE		CAUSE		EFFECT		
Serious	20	Negligence or Accident	5	Reparable	10	35
Serious	20	Negligence or Accident	5	Emergency	20	45
Serious	20	Negligence or Accident	5	Irreparable or Liable	30	55
Serious	20	Willful	10	Reparable	10	40
Serious	20	Willful	10	Emergency	20	50
Serious	20	Willful	10	Irreparable or Liable	30	60
Serious	20	Suspicious	20	Reparable	10	50
Serious	20	Suspicious	20	Emergency	20	60
Serious	20	Suspicious	20	Irreparable or Liable	30	70

MAGNITUDE		CAUSE		EFFECT		
Repeated Serious	30	Negligence or Accident	5	Reparable	10	45
Repeated Serious	30	Negligence or Accident	5	Emergency	20	55
Repeated Serious	30	Negligence or Accident	5	Irreparable or Liable	30	65
Repeated Serious	30	Willful	10	Reparable	10	50
Repeated Serious	30	Willful	10	Emergency	20	60
Repeated Serious	30	Willful	10	Irreparable or Liable	30	70
Repeated Serious	30	Suspicious	20	Reparable	10	60
Repeated Serious	30	Suspicious	20	Emergency	20	70
Repeated Serious	30	Suspicious	20	Irreparable or Liable	30	80

MAGNITUDE		CAUSE		EFFECT		
Willful Repeated	40	Negligence or Accident	5	Reparable	10	55
Willful Repeated	40	Negligence or Accident	5	Emergency	20	65
Willful Repeated	40	Negligence or Accident	5	Irreparable or Liable	30	75
Willful Repeated	40	Willful	10	Reparable	10	60
Willful Repeated	40	Willful	10	Emergency	20	70
Willful Repeated	40	Willful	10	Irreparable or Liable	30	80
Willful Repeated	40	Suspicious	20	Reparable	10	70
Willful Repeated	40	Suspicious	20	Emergency	20	80
Willful Repeated	40	Suspicious	20	Irreparable or Liable	30	90

MAGNITUDE		CAUSE		EFFECT		
Pervasive	50	Negligence or Accident	5	Reparable	10	65
Pervasive	50	Negligence or Accident	5	Emergency	20	75
Pervasive	50	Negligence or Accident	5	Irreparable or Liable	30	85
Pervasive	50	Willful	10	Reparable	10	70
Pervasive	50	Willful	10	Emergency	20	80
Pervasive	50	Willful	10	Irreparable or Liable	30	90
Pervasive	50	Suspicious	20	Reparable	10	80
Pervasive	50	Suspicious	20	Emergency	20	90
Pervasive	50	Suspicious	20	Irreparable or Liable	30	100

5.10.6.2 Administrative action.

Based on the above scoring, it is DWD's policy that the following corrective actions or disciplinary measures are **equitable and proportional responses** for dealing with a breach caused by an authorized user of a DWD-administered system:

ADMINISTRATIVE CONSEQUENCES TABLE	
MAGNITUDE, CAUSE, AND EFFECT ASSESSMENT RATING	CORRECTIVE OR DISCIPLINARY ACTION
20	If a supervisor's intercession, based on mitigating factors, reduces a "25" rating to a "20," the user may be let off with a verbal warning. The supervisor must justify the rating in writing and still must notify DWD TSU. This option is applicable only if the breached data remains in the possession or control of authorized users (for example, in an unencrypted email sent in-network to another user).
25–30	For State staff, a written reprimand will be issued to the user and copied to the DWD Assistant Director for Administration. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director.
35–40	For State staff, a written reprimand will be copied to DED HR and to the DWD Assistant Director for Administration. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director. ALL USERS receiving this assessment must undergo mandatory retraining on confidentiality procedures, be recertified, and re-sign the attestation form. The Supervisor should forward any recommendations for remedial measures or compliance assistance to TSU. Temporary reduction of level of authorized access (reduced to probationary access only).
45–60	For State staff, a written reprimand will be copied to DED HR and the DWD Assistant Director of Administration. For board staff or other subrecipients, an incident report will be forwarded to the Local WDB Executive Director. ALL USERS receiving this assessment must undergo mandatory retraining on confidentiality procedures, be recertified, and re-sign the attestation form. Temporary suspension of authorized access for a specific length of time (not to exceed two weeks), to be determined by the DWD TSU Manager.
65–80	For State staff, a written reprimand and notice of a concern will be copied to DED HR and the DWD Assistant Director for Administration. For board staff or other subrecipients, an incident report and notice of a concern will be forwarded to both the Local WDB Chair and the Local WDB Executive Director. The user will be permanently debarred from authorized access to DWD-administered systems. For State staff, potential reassignment of duties or reduction in grade if this loss of access affects the ability to perform one's current job.
85–100	Immediate debarment from authorized access to <u>all</u> DED systems. For State staff, a letter recommending dismissal for cause, per the DED Personal Accountability and Conduct Policy (2016-09-21), will be sent by the DWD Assistant Director for Administration to DED HR. For board staff or other subrecipients, an official notice of debarment will be sent to the Local WDB Chair and the Local WDB executive director. The DWD Assistant Director for Administration may instruct DWD Fiscal to conduct a compliance review to determine contract, funding, or award repercussions of the incident.

- 5.10.8 **Whistleblower clause**—All DED employees and DED system users should report any potential breach of confidentiality through their respective lines of supervision. If you feel that reporting any issue in that manner might adversely affect your job, you can report directly to the DWD Assistant Director for Administration at DWD Central Office. Any reported incident will be investigated by DWD Central Office staff or designee, and will be held in strictest confidence until the results are conclusive. Federal procurement law (41 U.S.C. 4712) prohibits reprisals for reporting violations of a law, rule, or regulation related to a federal award.
- 5.10.9 The SECMS is the official system of record, and the data therein is the official “data of record.” The Annual Agreement between DWD and its subrecipients specifies that if any subrecipient “uses any additional external data tracking system, it must have security protocols that are consistent with State standards, in order to safeguard any Personally Identifiable Information.” Confidential information or PII on a non-governmental or non-State (private or non-profit) computer system must be secure. The State holds subrecipients financially liable for breaches of information placed on unprotected systems. DWD’s Memorandum of Agreement with DES on the exchange, transfer, and/or release of computerized information provides that DWD will provide credit monitoring or privacy-protection services if compromised confidential information is accessed or disclosed in violation of that Agreement. DWD holds subrecipients accountable for that cost if they allow transfer of secure information to an unprotected computer system lacking adequate firewalls, anti-viral, or intrusion protection. (Creation and maintenance of systems without appropriate content filters are also disallowed expenditures. *See Section 7, “Federal Laws.”*) DWD will review access rights for such subrecipients.

5.11 Mitigation of a breach:

- 5.11.1 Remediation and mitigation procedures that are allowable, prior to approval by the DWD Assistant Director for Administration, include:
- Redaction or deletion of sent and received email. Permanent images of such files will remain in the master email server database. However, redaction or deletion will prevent the information from being sent again inadvertently, or forwarded.
 - Tightening local physical security, such as at workstation cubicles, secure file safes or cabinets, and other parts of the premises. Floor-plan adjustments may need to be made to keep display screens out of public line-of-sight. Physical access to printers, copiers, scanners, etc., may need to be restricted. State and local monitors may look for these precautions in their regular monitoring visits.
- 5.11.2 Other than the redaction or deletion of emails exchanged wholly within the sphere of authorized users, and modification of habits, procedures, or methods that led to the breach, **no data affected by a breach is to be deleted or modified except under the direction of DWD Assistant Director for Administration.**
- 5.11.3 Notification Trigger and Timing — The requirement to notify a customer is generally triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person. DWD will provide notifications to customers, if warranted, regarding the occurrence of an information breach, per Section 5.9.5.1. **Unauthorized or premature discussion of a breach with a customer is itself a breach of confidentiality.** (State law also provides an option for *delaying notification* of affected customers if that notification might alert a suspect and jeopardize an investigation of the incident by law enforcement.)

6. INFORMED CONSENT AND PERMISSIVE DISCLOSURES

- 6.1 The procedures for handling confidential UC information in UC Wage Records are dictated by 20 CFR Part 603 (*see Attachment 3 to the accompanying Issuance*). Adherence to these procedures is formalized by an agreement between DES and DWD, and by contract between DWD and each LWDA. Part 603's provisions include:
- 6.1.2 Disclosure of confidential UC information through **informed consent** is permissible to an **agent** whom an individual or an employer has empowered. However, the agent must present a **written, signed release** from the individual or employer the agent represents. (The State may accept an electronically submitted release *if* the State is satisfied that the release is authentic.)
- 6.1.2.1 When a written release is impossible or impracticable to obtain, the agent may present another form of consent as permitted by the State UC agency in accordance with State law (e.g., a Power of Attorney or Durable Power of Attorney for an attorney-*in-fact*).
- 6.1.2.2 An elected official performing **constituent services** [e.g., a State legislator acting on behalf of a person or business resident in that legislator's district], may act as an agent. The official must present *reasonable evidence*⁵⁰ (such as a **letter** from the individual or employer requesting assistance, or a **written record** of a telephone request from the individual or employer) that the individual or employer has authorized such disclosure.
- 6.1.2.3 A licensed attorney (attorney-*at-law*) retained for purposes related to the State's UC law is also an agent when representing the individual or employer.
- 6.1.3 Disclosures to any other third party (other than an agent) or any ongoing disclosures (e.g., regular reports to another agency) of confidential information require a *written release* and are limited in scope.
- 6.1.3.1 The release must be **signed** by the individual or employer to whom the information pertains. It must specifically identify the information to be disclosed. It must acknowledge that State government files will be accessed to obtain that information. It must declare the specific purpose(s) for which the information is sought. It must stipulate that information obtained under the release will be used only for the declared purpose(s) and disclose all the parties who might receive the information. The declared purpose in the release must be limited to:
- providing a service or benefit to the individual signing the release; or
 - administration/evaluation of a program to which the release pertains.
- 6.1.3.2 Electronic signatures on consent forms may be accepted.⁵¹ However, if any question exists about the authenticity of the electronic signature, DWD TSU may be consulted before accepting it.
- 6.1.4 DWD TSU will provide written procedures for release of information and an accompanying release form. These must be used for all transactions.

⁵⁰ 20 CFR 603.5(d)(1)(ii).

⁵¹ 20 CFR 630.5(d); RSMo 432.230.

6.2 A jobseeker customer (if a youth, the parents or legal guardian) has a right to request and receive a copy of the contents of the **service notes** in the customer's case file.^{52, 53}

6.2.1 Never capture and deliver personally requested information to an individual, agent, or third party by means of a SECMS PRINT-SCREEN command, PDF conversion, clipping tool, or similar means. The formatting, coding, or proprietary information on the case-management screen or file is not to be conveyed. Copy and paste, or transcribe, the customer's desired personal information into a neutral medium before presenting to the customer or agent.

6.2.2 The customer *does not necessarily have a right to all* information located in case-management or file records. Information that the customer did not **personally disclose** for inclusion in that file or record is **confidential** from the customer. For example, information regarding that customer that originated with, or was created by, another agency, partner, or contractor is not disclosable to the customer.

6.3 In keeping with Section 552a(c) of the Privacy Act of 1974, as amended, an accounting of all disclosures of any confidential record to any person or agency (including the customer) must be kept for a period of five years, or the life of the customer's record, whichever is longer. This accounting should include the name and address of any requestor as well as the date, nature, and purpose of each disclosure request. Denied requests and the cause for denial must be included in this accounting. The SECMS may be used for this purpose.

⁵² DWD Issuance 02-2017, "Statewide Case Note Policy," August 11, 2017. (This right is also established by the Privacy Act of 1974, as amended, Pub. Law 93-579 [5 U.S.C. 552a(d)], with which subrecipients must comply.

⁵³ Missouri State law also provides that "upon receipt of a written request from a claimant or his or her authorized representative, the [Division of Employment Security] shall supply information previously submitted to the division by the claimant, the claimant's wage history, and the claimant's benefit payment history." RSMo 288.250.

7. LEGAL, REGULATORY, AND POLICY REFERENCES

The following federal and state legal provisions may affect the programs and services offered through the local workforce investment system. This list is not exhaustive. Varieties of civil and criminal provisions surround confidential information or identity theft and may apply to this Plan.

- Federal laws
 - Workforce Innovation and Opportunity Act, Pub. L. 113-128 [29 U.S.C. 3101 et seq.].
 - Workforce Innovation and Opportunity Act (WIOA), Section 188, “Nondiscrimination,” Pub. Law 113-128 [29 U.S.C. 3248] and implementing regulations at 29 CFR Part 38.
 - The Family Educational Rights and Privacy Act of 1974 (FERPA), Pub. Law 93-380, August 21, 1974 (20 U.S.C. 1232g)—Protects the privacy interests of students and parents of students who are minors with respect to their personal education records. FERPA is reinforced by Missouri State law,⁵⁴ which prescribes substantial civil monetary penalties for violation of the confidentiality of certain education records and student privacy.
 - Section 504 of the Rehabilitation Act of 1973, “Nondiscrimination under Federal Grants,” Pub. Law 93-112 [29 U.S.C. 701 et seq.] as amended, including amendments made by the ADA Amendments Act of 2008, Pub. Law 110-325 [42 U.S.C. 12101 et seq.] and implementing regulations at 29 CFR part 32.
 - The Privacy Act of 1974, as amended, Pub. Law 93-579 [5 U.S.C. 552a]. Principally addresses the contents and disclosure procedures for records kept by federal agencies, as well as individuals’ access to those records. However, some federal awards and grants require recipient’s assurances to abide by certain requirements or procedures in the Act.
 - Pub. Law 105-318, “Identity Theft Assumption and Deterrence Act” [18 U.S.C. 1028].
 - The Federal Information Security Modernization Act of 2014 (FISMA), Pub. Law 113-283 [44 U.S.C. Chapter 35]. FISMA became law after passage of WIOA. Its information-security provisions apply specifically to federal operations and assets. However, some federal awards and grants may require a recipient’s contractual assurances to abide by certain requirements or procedures in the Act.
 - The Federal Funding Accountability and Transparency Act of 2006 (FFATA),⁵⁵ as amended by the Digital Accountability and Transparency Act of 2014 (DATA Act),⁵⁶ specifies federal standards for data elements for public accountability and transparency purposes.
 - The Consolidated Appropriations Act of 2016⁵⁷ stipulates that no federal funds may be used to maintain or establish a computer network unless such network blocks the viewing, downloading, and exchanging of pornography. That is, the creation or maintenance of any network without appropriate content filters is a disallowed cost.

⁵⁴ RSMo 161.096.5.

⁵⁵ Pub. Law 110-252.

⁵⁶ Pub. Law 113-101.

⁵⁷ Pub. Law 114-113, Section 521(a), December 18, 2015.

- Federal regulations
 - Uniform Guidance for Federal Awards, 2 CFR 200.303, “Internal controls,” and 2 CFR 200.337, “Restrictions on public access to records.”
 - Uniform Guidance for Federal Awards, 2 CFR 200.113, “Mandatory disclosures.”
 - 20 CFR Part 603, “Confidentiality and Disclosure of State UC Information”;
 - 34 CFR Part 99, “Family Educational Rights and Privacy”;
 - 34 CFR 361.38, “Protection, Use, and Release of Personal Information”
 - 20 CFR 683.220(a) “What are the internal controls requirements for recipients and subrecipients of Workforce Innovation and Opportunity Act title I and Wagner-Peyser Act funds?”
 - 20 CFR 658.411 “Action on complaints.”
 - 20 CFR 683.600 “What local area, State, and direct recipient grievance procedures must be established?”
- Federal guidance and standards
 - U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) 5-08, “Policy for Collection and Use of Workforce System Participants’ Social Security Numbers,” November 13, 2008.
 - The protection, use, and release of personal information under the Vocational Rehabilitation (VR) program, which is one of the core programs under WIOA, are governed by 34 CFR 361.38, listed above. In addition to these VR program-specific confidentiality requirements, VR agencies also must consider FERPA and UC confidentiality requirements when accessing confidential UC information in wage records and PII from education records. On August 23, 2016, DOL and ED issued joint guidance authorizing matching of PII in education records, vocational rehabilitation records, and wages records used for administering UC. (U.S. Department of Labor, Training and Employment Administration, Training and Employment Guidance Letter 7-16, “Data Matching to Facilitate WIOA Performance Reporting,” Attachment 1, “Joint Guidance with the Department of Education for Matching PII From Educational Records and Personal Information from Vocational Rehabilitation Records with Unemployment Compensation Wage Records”).
 - National Institute of Standards and Technology (NIST), FIPS Pub 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.
 - OMB, Revision of OMB Circular A-130, Managing Federal Information as a Strategic Resource (Washington, D.C.; July 28, 2016).
 - U.S. Department of Labor, Employment and Training Administration, Training and Employment Guidance Letter (TEGL) No. 39-11, “Guidance on the Handling and Protection of Personally Identifiable Information (PII),” June 28, 2012 (*see Attachment 4*).
 - U.S. Department of Education “Data Breach Response Checklist,” PTAC-CL, September 2012.
 - U.S. Department of Education, Departmental Directive OM:6-107, April 15, 2008, “External Breach Notification Policy and Plan.”
 - National Institute of Standards and Technology, FIPS Pub 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004.

- Missouri State laws
 - Revised Statutes of Missouri, Chapter 288, Section 250, Title XVIII, DOLIR; also Chapter 407, Section 407.1500, "Merchandising Practices" (requires customer PII-breach notification, including PII held by governmental agencies).
 - Missouri's Safe at Home Act (2007) RSMo 589.660–589.683, provides for strict address confidentiality for program participants who are experiencing domestic abuse or have similar reasons for relocation to secure locations.
 - RSMo 37.070, "Transparency policy—public availability of data—broad interpretation of sunshine law requests—breach of the public trust, when."
 - RSMo 576.020 "Public servant acceding to corruption—penalty."
 - RSMo 576.050, "Misuse of public information—penalty."
- DED/DWD Policies
 - DED "Acceptable Computer Use Policy," July 7, 2017.
 - DED "Personal Accountability and Conduct" policy, September 21, 2016.
 - Applicable DWD Policy Issuances are available at <https://jobs.mo.gov/dwdissuances>

8. ACRONYMS USED IN THIS GUIDE

AEL	Missouri Adult Education and Literacy Program (DESE)
APPID	Applicant ID
CBHE	Missouri Coordinating Board for Higher Education
CEO	Chief Elected Official of an LWDA
CFR	<i>Code of Federal Regulations</i>
DATA Act	Digital Accountability and Transparency Act of 2014
DED	Missouri Department of Economic Development
DES	Missouri Division of Employment Security (DOLIR)
DESE	Missouri Department of Elementary and Secondary Education
DOB	Date of Birth
DOC	Missouri Department of Corrections
DOL	U.S. Department of Labor
DOLIR	Missouri Department of Labor and Industrial Relations
DSS	Missouri Department of Social Services
DWD	Missouri Division of Workforce Development (DED)
ED	U.S. Department of Education
ETA	Employment and Training Administration (<i>also</i> DOLETA; DOL)
FEIN	Federal Employer Identification Number
FERPA	Family Educational Rights and Privacy Act
FFATA	Federal Funding Accountability and Transparency Act of 2006
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act of 2014
FR	<i>Federal Register</i>
FSD	Missouri Family Support Division (DSS)
HSS	Missouri Department of Health and Senior Services
IP	Intellectual Property
ITSD	Missouri Information Technology Support Division (OA)
LFA	Local Fiscal Agent
Local WDB	Local Workforce Development Board
LWDA	Local Workforce Development Area
NAICS	North American Industrial Classification System
NIST	National Institute of Standards and Technology
NRS	National Reporting System
OA	Missouri Office of Administration
OMB	Federal Office of Management and Budget
PII	Personally Identifiable Information
RSB	Missouri Rehabilitation Services for the Blind (DSS/FSD)
RSMo	<i>Revised Statutes of the State of Missouri</i>
SAOP	Senior Agency Official for Privacy
SECMS	statewide electronic case-management system (This is a generic term; an official name will be assigned when the new system goes online in 2017.)
SSA	Social Security Act (<i>also</i> , Social Security Administration)
SSN	Social Security Number
TEGL	Training and Employment Guidance Letter (DOL/ETA)
TSU	Technical Support Unit (DWD)
U.S.C.	<i>United States Code</i>
UAF	User Attestation Form
UC	Unemployment Compensation
UI	Unemployment Insurance
VR	Missouri Vocational Rehabilitation (DESE)
WIOA	Workforce Innovation and Opportunity Act
WOTC	Work Opportunity Tax Credit
WIPS	Workforce Integrated Performance System
WRIS	Wage Record Interchange System



CONFIDENTIAL INFORMATION USER ATTESTATION FORM

I understand that in the course of my employment with the Missouri Division of Workforce Development, Local Workforce Development Board, subrecipient, or partner agency, I will receive or become aware of information that is sensitive or confidential. This information may be written, electronic, or verbal, and come from a variety of sources. I understand that I am not to access sensitive or confidential information unless it is necessary in order for me to complete my job responsibilities. I further understand that the Missouri Division of Workforce Development's policy on Confidentiality and Information Security applies to information I may inadvertently hear or see that does not directly involve me in an official capacity. I acknowledge that I must protect all sensitive or confidential information.

I understand that in the performance of my duties I may be requested to provide sensitive or confidential information to others. I agree to hold in confidence and not to disclose any sensitive or confidential information to any person, including employees of state, federal, or local governments, except to those who have an official business reason for the information. Should I have questions regarding the proper handling and disclosure of confidential or sensitive information, I will immediately notify my supervisor for further clarification and direction prior to releasing the information.

I understand that this prohibition against improper disclosure of sensitive or confidential information that I receive or become aware of in the course of my employment persists and continues after the termination of that employment. If I willfully and knowingly disclose such information in any manner to any person or agency not entitled to receive information, I understand that I may be subject to adverse action, including corrective or disciplinary action, or possibly, civil or criminal personal liability.

I further understand that changing circumstances may cause the Missouri Division of Workforce Development to further revise its Confidentiality and Information Security Plan. In response to notification of policy revisions, I will review the most current Confidentiality and Information Security policy, available on *jobs.mo.gov*, and discuss any questions or concerns I may have with my supervisor or a human resources representative.

I acknowledge that I have received the mandatory training and have read, understand, and will adhere to the Missouri Division of Workforce Development's Confidentiality and Information Security Plan and the above requirements.

Signature _____

Print Name _____

Employer of Record _____

Date Signed _____

The Missouri Division of Workforce Development is an equal opportunity employer/program.
Auxiliary aids and services are available upon request to individuals with disabilities.
Missouri Relay Services at 711.

Page 34 of 34



POLICY STATEMENT

Subject: Acceptable Computer Use	Issued: 03/16/05	Policy Section: HR
	Revised: 07/07/17	Page: 1 of 5
	Reviewed: 07/07/2017	

As a result of their employment, Department of Economic Development (DED) employees may receive access to various electronic devices, including a personal computer with approved software programs, print capabilities, an electronic mail system and internet access, to assist them in conducting state business. All such electronic devices and related applications, including email and internet access, are provided exclusively for business-related use; any personal use of these devices is restricted as set forth in this policy. Employee access to technology is a privilege that requires individual users to act responsibly.

The state system includes all electronic devices or applications provided to DED employees to perform a job-related function, regardless of whether or not DED directly provided the device or program.

“State system[s] includes, but is not limited to: desktop and laptop computers, personal data assistants, telephones, printers, fax machines, scanners, copiers, electronic communications, VPN, and internet access.

Scope:

This policy applies to all DED employees and/or state system users, regardless of whether system use occurs on state property. This policy cannot be modified by a supervisor’s statement or conduct.

Resources:

- Harassment and Discrimination Policy
- Sunshine Law Policy
- Records Disposition Schedule
- United States Copyright Law – www.copyright.gov/title17/circ92.pdf

Legal Guidelines:

1. No state system, as defined in this policy, shall be used to create, send, receive, view or store any message and/or attachment that may violate any local, state or federal law or that contains inappropriate, offensive, harassing, derogatory or disruptive content of any kind, including but not limited to content regarding: Race, National Origin, Religious Belief, Disability, Gender, Age, Sexual Orientation, Sexual Implications, Profanity, Obscenities or Inappropriate Language.
2. DED strictly prohibits use of state systems to access web sites containing offensive, harassing or disruptive content, including, but not limited to content regarding sexual implications, racial slurs, gender specific derogatory statements or any other offensive comment regarding gender, race, age, sexual orientation, religious belief, national origin or disability.



POLICY STATEMENT

Subject: Acceptable Computer Use	Issued: 03/16/05	Policy Section: HR
	Revised: 07/07/17	Page: 2 of 5
	Reviewed: 07/07/2017	

3. Copyright Infringement is prohibited. Employees who download copyrighted material must do so in compliance with any agreements posted by the content's author and pursuant to current copyright law. If an employee is unsure of the work's copyright, patent or other ownership status, the employee shall not post, upload, download or otherwise use the work. Employees must give credit to owners or originators of any material used or transmitted via state systems.

User Conditions

Account(s) – State	As a result of their employment, DED employees may be provided with a state or other email account. Employees shall use any such accounts exclusively for state business and in compliance with this policy.
Games & Greeting Cards	Employees are <u>prohibited</u> from loading/playing games or sending electronic greeting cards.
Lost Equipment	Any state-owned personal computer, personal communication device or peripheral equipment that is lost or stolen <u>must be</u> reported immediately to the employee's supervisor and ITSD.
Personal Use	<ul style="list-style-type: none"> ▪ Personal use <u>must not</u> violate any of the provisions of this policy, including, but not limited to, all Legal Guidelines. ▪ Personal use of computers <u>is not</u> permitted during employee breaks. ▪ Personal use is permitted one hour before and one hour after an employee's work hours with the supervisor's approval; however, this may not result in the building being occupied outside of normal operations. ▪ Personal use is permitted during an employee's scheduled meal. ▪ If an employee is authorized to remove or access systems outside of the work location and/or business hours – the access shall not be for personal reasons. ▪ Employees <u>are not</u> permitted to connect any unauthorized item to a state-issued item.. Examples include but are not limited to: flash-drive, camera, IPOD, IPAD, cellular phone. This restriction includes recharging items.
Printing	Employees are <u>not</u> permitted to utilize DED equipment to print personal items.
Privacy	<ul style="list-style-type: none"> ▪ Employee use of state systems is neither personal nor private. No employee shall have a presumption or any reasonable expectation of



POLICY STATEMENT

Subject: Acceptable Computer Use	Issued: 03/16/05	Policy Section: HR
	Revised: 07/07/17	Page: 3 of 5
	Reviewed: 07/07/2017	

	<p>privacy in:</p> <ul style="list-style-type: none"> ○ the content of any electronic documents (including word processing documents, emails, cookies, bookmarks, etc.) located on the computer's hard drive or assigned server space; or ○ information sent, received or accessed through the state network. <ul style="list-style-type: none"> ▪ Employees waive any expectation of privacy in records created, sent, received, accessed or stored in connection with the use of state systems. DED may monitor employee use of state systems at any time and without notice. Such monitoring may occur in response to suspected violations of the Acceptable Computer Use Policy, at the conclusion of an employee's probationary period, randomly, or for any reason that DED deems appropriate. ▪ Authorized department staff (managers, supervisors, certain human resources employees and legal counsel) may, with or without cause, access an employee's hard drive and/or assigned server space to ascertain compliance with this, or any other, policy, regulation, or law.
Retention of Records	<ul style="list-style-type: none"> ▪ All records created, sent, received, accessed or stored in connection with the use of state systems shall be retained pursuant to the department's Sunshine Law Policy and the applicable Records Retention Disposition Schedule(s), both available on DED's intranet. ▪ If an employee engages in personal use of state systems, any records created, sent, received, accessed or stored in the course of such use shall be retained as outlined in the department and/or division record disposition schedules(s) and/or the department's Sunshine Law Policy, available on the DED intranet.
Signature Blocks	<ul style="list-style-type: none"> ▪ Signature blocks are limited to pertinent sender contact information limited to: title, work address, work phone and/or fax number, and employment related social media icons. ▪ Employees are prohibited from including quotes, graphics and/or taglines in email signatures. ▪ The Department Director may temporarily authorize specialized signature blocks to promote Departmental events (e.g. Governor's Conference).



POLICY STATEMENT

Subject: Acceptable Computer Use	Issued: 03/16/05	Policy Section: HR
	Revised: 07/07/17	Page: 4 of 5
	Reviewed: 07/07/2017	

Social Media	<ul style="list-style-type: none"> ▪ Employees are <u>prohibited</u> from posting on their personal online sites information or communications that could be attributed to the department or appear to be endorsed by or to have originated from the department. ▪ Employees are <u>prohibited</u> from linking from their personal social media sites to the department's internal or external web site(s). An employee may not speak on behalf of the department or represent that they are speaking on behalf of the department using any social media unless authorized by their Division Director. ▪ An employee may be approved by his/her Division Director to utilize professional social networks websites, including but not limited to Facebook, Twitter, LinkedIn and YouTube for DED business purposes. ▪ The following guidelines apply when posting authorized material on behalf of the Department: <ul style="list-style-type: none"> ○ Employees are prohibited from disclosing confidential information. Disclosing confidential information, even unintentionally, can result in legal action against you and the department. ○ Posts should be based upon position assignment, accurate, professional, meaningful and respectful. ○ Employees are responsible for correcting any errors or mistakes immediately and indicating the information has been corrected, if necessary.
Software	Only ITSD is authorized to install/download software.
Streaming: Business Related	Employees may, with supervisory authorization, listen or view business-related content through audio/visual streaming.
Streaming: Non-Business Related	Employees <u>are not</u> permitted to stream audio and/or visual material that is not directly related to his/her position responsibilities or Departmental business.
Suspicious or Unwanted Activity	<ul style="list-style-type: none"> ▪ Employees <u>should not</u> open suspicious emails or contact from an unknown source. Suspicious email should be deleted from the inbox and from the deleted inbox. Employees may contact ITSD if they receive suspicious electronic communications. ▪ Employees should notify his/her supervisor if he/she continues to receive unwanted activity that may violate the policy. ▪ <u>DO NOT FORWARD SUSPICIOUS EMAILS TO SUPERVISORS,</u>



POLICY STATEMENT

Subject: Acceptable Computer Use	Issued: 03/16/05	Policy Section: HR
	Revised: 07/07/17	Page: 5 of 5
	Reviewed: 07/07/2017	

	<u>COWORKERS or HUMAN RESOURCES and subject another user to corruption.</u>
User ID	<ul style="list-style-type: none"> ▪ Each employee is responsible for all computer and internet use associated with his or her assigned user ID or on any device issued to the employee. ▪ Employees are <u>prohibited</u> from using another individual's user ID and confidential password without authorization. ▪ An employee <u>shall not</u> give his or her user ID and/or password to any other individual and must take reasonable measures to guard against unauthorized access to his or her assigned equipment or accounts.
Wallpaper	<ul style="list-style-type: none"> ▪ Employees may use personal pictures as wallpaper on computer desktops. ▪ Employees may open a picture attachment from a personal email account and save the picture as their wallpaper.
Websites	<p>ITSD uses software to categorize web traffic and block access to sites that may compromise the state system (e.g. spyware, phishing).</p> <ul style="list-style-type: none"> ▪ Employees <u>shall not</u> make any attempts to circumvent ITSD blocked access to access a blocked website. ▪ If an employee believes he/she needs access to a blocked website, the employee must submit an ITSD online helpdesk ticket and notify his/her supervisor.

Policy Violation

1. Violation of this policy may result in disciplinary action up to and including termination, depending on the circumstances and severity of the behavior.
2. Employees who violate this policy may also be subject to prosecution under state or federal law. Under appropriate circumstances, the department may refer suspected violations of law to appropriate law enforcement authorities and provide investigators with access to data contained on state systems, as permitted by law.
3. If DED discovers any material that violates this policy on an employee's computer, ITSD will remove the offending item and notify human resources.
4. DED may conduct periodic audits to detect unauthorized software and hardware to ensure compliance with this policy. In the case of non-compliance, any and all fees, penalties, or fines will be the responsibility of the employee accountable for committing the violation(s).

CFR Title 20: Employees' Benefits (reprinted from the *electronic Code of Federal Regulations*)

**PART 603—FEDERAL-STATE UNEMPLOYMENT COMPENSATION (UC) PROGRAM;
CONFIDENTIALITY AND DISCLOSURE OF STATE UC INFORMATION**
(as amended by the *Workforce Innovation and Opportunity Act*)

Contents

Subpart A—In General

- §603.1 What are the purpose and scope of this part?
- §603.2 What definitions apply to this part?

Subpart B—Confidentiality and Disclosure Requirements

- §603.3 What is the purpose and scope of this subpart?
- §603.4 What is the confidentiality requirement of Federal UC law?
- §603.5 What are the exceptions to the confidentiality requirement?
- §603.6 What disclosures are required by this subpart?
- §603.7 What requirements apply to subpoenas, other compulsory processes, and disclosure to officials with subpoena authority?
- §603.8 What are the requirements for payment of costs and program income?
- §603.9 What safeguards and security requirements apply to disclosed information?
- §603.10 What are the requirements for agreements?
- §603.11 How do States notify claimants and employers about the uses of their information?
- §603.12 How are the requirements of this part enforced?

Subpart C—Mandatory Disclosure for Income and Eligibility Verification System (IEVS)

- §603.20 What is the purpose and scope of this subpart?
- §603.21 What is a requesting agency?
- §603.22 What information must State UC agencies disclose for purposes of an IEVS?
- §603.23 What information must State UC agencies obtain from other agencies, and crossmatch with wage information, for purposes of an IEVS?

AUTHORITY: Secs. 116, 189, 503, Pub. L. 113-128, 128 Stat. 1425 (Jul. 22, 2014); 20 U.S.C 1232g.

SOURCE: 71 FR 56842, Sept. 27, 2006, unless otherwise noted.

Subpart A—In General

§603.1 What are the purpose and scope of this part?

The purpose of this part is to implement the requirements of Federal UC law concerning confidentiality and disclosure of UC information. This part applies to States and State UC agencies, as defined in §603.2(f) and (g).

§603.2 What definitions apply to this part?

For the purposes of this part:

- (a)
 - (1) *Claim information* means information about:
 - (i) Whether an individual is receiving, has received, or has applied for UC;
 - (ii) The amount of compensation the individual is receiving or is entitled to receive; and
 - (iii) The individual's current (or most recent) home address.

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

- (2) For purposes of subpart C (IEVS), claim information also includes:
 - (i) Whether the individual has refused an offer of work and, if so, a description of the job offered including the terms, conditions, and rate of pay; and
 - (ii) Any other information contained in the records of the State UC agency that is needed by the requesting agency to verify eligibility for, and the amount of, benefits.
- (b) *Confidential UC information* and *confidential information* mean any UC information, as defined in paragraph (j) of this section, required to be kept confidential under §603.4.
- (c) *Public domain information* means—
 - (1) Information about the organization of the State and the State UC agency and appellate authorities, including the names and positions of officials and employees thereof;
 - (2) Information about the State UC law (and applicable Federal law) provisions, rules, regulations, and interpretations thereof, including statements of general policy and interpretations of general applicability; and
 - (3) Any agreement of whatever kind or nature, including interstate arrangements and reciprocal agreements and any agreement with the Department of Labor or the Secretary, relating to the administration of the State UC law.
- (d) *Public official* means:
 - (1) An official, agency, or public entity within the executive branch of Federal, State, or local government who (or which) has responsibility for administering or enforcing a law, or an elected official in the Federal, State, or local government.
 - (2) Public postsecondary educational institutions established and governed under the laws of the State. These include the following:
 - (i) Institutions that are part of the State's executive branch. This means the head of the institution must derive his or her authority from the Governor, either directly or through a State WDB, commission, or similar entity established in the executive branch under the laws of the State.
 - (ii) Institutions which are independent of the executive branch. This means the head of the institution derives his or her authority from the State's chief executive officer for the State education authority or agency when such officer is elected or appointed independently of the Governor.
 - (iii) Publicly governed, publicly funded community and technical colleges.
 - (3) Performance accountability and customer information agencies designated by the Governor of a State to be responsible for coordinating the assessment of State and local education or workforce training program performance and/or evaluating education or workforce training provider performance.
 - (4) The chief elected official of a local area as defined in WIOA sec. 3(9).
 - (5) A State educational authority, agency, or institution as those terms are used in the Family Educational Rights and Privacy Act, to the extent they are public entities.
- (e) *Secretary* and *Secretary of Labor* mean the cabinet officer heading the United States Department of Labor, or his or her designee.
- (f) *State* means a State of the United States of America, the District of Columbia, the Commonwealth of Puerto Rico, and the United States Virgin Islands.
- (g) *State UC agency* means an agency charged with the administration of the State UC law.
- (h) *State UC law* means the law of a State approved under Section 3304(a) of the Internal Revenue Code of 1986 (26 U.S.C. 3304(a)).
- (i) *Unemployment compensation* (UC) means cash benefits payable to individuals with respect to their unemployment.
- (j) *UC information* and *State UC information* means information in the records of a State or State UC agency that pertains to the administration of the State UC law. This term includes those State wage reports collected under the IEVS (Section 1137 of the Social Security Act (SSA)) that are obtained by the State UC agency for determining UC monetary eligibility or are downloaded to the State UC agency's files as a result of a crossmatch but does not otherwise include those wage reports. It does not include information in a State's

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

Directory of New Hires, but does include any such information that has been disclosed to the State UC agency for use in the UC program. It also does not include the personnel or fiscal information of a State UC agency.

- (k) *Wage information* means information in the records of a State UC agency (and, for purposes of §603.23 (IEVS)), information reported under provisions of State law which fulfill the requirements of Section 1137, SSA) about the—
- (1) Wages paid to an individual,
 - (2) Social security account number (or numbers, if more than one) of such individual, and
 - (3) Name, address, State, and the Federal employer identification number of the employer who paid such wages to such individual.

[71 FR 56842, Sept. 27, 2006, as amended at 81 FR 56333, Aug. 19, 2016]

Subpart B—Confidentiality and Disclosure Requirements

§603.3 What is the purpose and scope of this subpart?

This subpart implements the basic confidentiality requirement derived from Section 303(a)(1), SSA, and the disclosure requirements of Sections 303(a)(7), (c)(1), (d), (e), (h), and (i), SSA, and Section 3304(a)(16), Federal Unemployment Tax Act (FUTA). This subpart also establishes uniform minimum requirements for the payment of costs, safeguards, and data-sharing agreements when UC information is disclosed, and for conformity and substantial compliance with this proposed rule. This subpart applies to States and State UC agencies, as defined in §603.2(f) and (g), respectively.

§603.4 What is the confidentiality requirement of Federal UC law?

- (a) *Statute.* Section 303(a)(1) of the SSA (42 U.S.C. 503(a)(1)) provides that, for the purposes of certification of payment of granted funds to a State under Section 302(a) (42 U.S.C. 502(a)), State law must include provision for such methods of administration as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due.
- (b) *Interpretation.* The Department of Labor interprets Section 303(a)(1), SSA, to mean that “methods of administration” that are reasonably calculated to insure the full payment of UC when due must include provision for maintaining the confidentiality of any UC information which reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with other publicly available information to reveal any such particulars, and must include provision for barring the disclosure of any such information, except as provided in this part.
- (c) *Application.* Each State law must contain provisions that are interpreted and applied consistently with the interpretation in paragraph (b) of this section and with this subpart, and must provide penalties for any disclosure of confidential UC information that is inconsistent with any provision of this subpart.

§603.5 What are the exceptions to the confidentiality requirement?

The following are exceptions to the confidentiality requirement. Disclosure of confidential UC information is permissible under the exceptions in paragraphs (a) through (g) of this section only if authorized by State law and if such disclosure does not interfere with the efficient administration of the State UC law. Disclosure of confidential UC information is permissible under the exceptions in paragraphs (h) and (i) of this section without such restrictions.

- (a) *Public domain information.* The confidentiality requirement of §603.4 does not apply to public domain information, as defined at §603.2(c).
- (b) *UC appeals records.* Disclosure of appeals records and decisions, and precedential determinations on coverage of employers, employment, and wages, is permissible provided all social security account numbers have been removed and such disclosure is otherwise consistent with Federal and State law.

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

- (c) *Individual or employer.* Disclosure for non-UC purposes, of confidential UC information about an individual to that individual, or of confidential UC information about an employer to that employer, is permissible.
 - (d) *Informed consent.* Disclosure of confidential UC information on the basis of informed consent is permissible in the following circumstances—
 - (1) *Agent*—to one who acts for or in the place of an individual or an employer by the authority of that individual or employer if—
 - (i) In general—
 - (A) The agent presents a written release (which may include an electronically submitted release that the State determines is authentic) from the individual or employer being represented;
 - (B) When a written release is impossible or impracticable to obtain, the agent presents such other form of consent as is permitted by the State UC agency in accordance with State law;
 - (ii) In the case of an elected official performing constituent services, the official presents reasonable evidence (such as a letter from the individual or employer requesting assistance or a written record of a telephone request from the individual or employer) that the individual or employer has authorized such disclosure; or
 - (iii) In the case of an attorney retained for purposes related to the State’s UC law, the attorney asserts that he or she is representing the individual or employer.
 - (2) *Third party (other than an agent) or disclosure made on an ongoing basis*—to a third party that is not acting as an agent or that receives confidential information following an informed consent disclosure on an ongoing basis (even if such entity is an agent), but only if that entity obtains a written release from the individual or employer to whom the information pertains.
 - (i) The release must be signed and must include a statement—
 - (A) Specifically identifying the information that is to be disclosed;
 - (B) That State government files will be accessed to obtain that information;
 - (C) Of the specific purpose or purposes for which the information is sought and a statement that information obtained under the release will only be used for that purpose or purposes; and
 - (D) Indicating all the parties who may receive the information disclosed.
 - (ii) The purpose specified in the release must be limited to—
 - (A) Providing a service or benefit to the individual signing the release that such individual expects to receive as a result of signing the release; or
 - (B) Carrying out administration or evaluation of a public program to which the release pertains.
- NOTE TO PARAGRAPH (d): The Electronic Signatures in Global and National Commerce Act of 2000 (E-Sign), Pub. L. 106-229, may apply where a party wishes to effectuate electronically an informed consent release (§603.5(d)(2)) or a disclosure agreement (§603.10(a)) with an entity that uses informed consent releases. E-Sign, among other things, sets forth the circumstances under which electronic signatures, contracts, and other records relating to such transactions (in lieu of paper documents) are legally binding. Thus, an electronic communication may suffice under E-Sign to establish a legally binding contract. The States will need to consider E-Sign’s application to these informed consent releases and disclosure agreements. In particular, a State must, to conform and substantially comply with this regulation, assure that these informed consent releases and disclosure agreements are legally enforceable. If an informed consent release or disclosure agreement is to be effectuated electronically, the State must determine whether E-Sign applies to that transaction, and, if so, make certain that the transaction satisfies the conditions imposed by E-Sign. The State must also make certain that the electronic transaction complies with every other condition necessary to make it legally enforceable.
- (e) *Public official.* Disclosure of confidential UC information to a public official for use in the performance of his or her official duties is permissible.
 - (1) “Performance of official duties” means administration or enforcement of law or the execution of the official responsibilities of a Federal, State, or local elected official. Administration of law includes research related to the law administered by the public official. Execution of official responsibilities does not include solicitation of contributions or expenditures to or on behalf of a candidate for public or political office or a political party.

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

(2) For purposes of §603.2(d)(2) through (5), “performance of official duties” includes, in addition to the activities set out in paragraph (e)(1) of this section, use of the confidential UC information for the following limited purposes:

- (i) State and local performance accountability under WIOA sec. 116, including eligible training provider performance accountability under WIOA secs. 116(d) and 122;
- (ii) The requirements of discretionary Federal grants awarded under WIOA; or
- (iii) As otherwise required for education or workforce training program performance accountability and reporting under Federal or State law.

- (f) *Agent or contractor of public official.* Disclosure of confidential UC information to an agent or contractor of a public official to whom disclosure is permissible under paragraph (e) of this section.
- (g) *Bureau of Labor Statistics.* The confidentiality requirement does not apply to information collected exclusively for statistical purposes under a cooperative agreement with the Bureau of Labor Statistics (BLS). Further, this part does not restrict or impose any condition on the transfer of any other information to the BLS under an agreement, or the BLS’s disclosure or use of such information.
- (h) *Court order; official with subpoena authority.* Disclosure of confidential UC information in response to a court order or to an official with subpoena authority is permissible as specified in §603.7(b).
- (i) *UC Program Oversight and Audits.* The confidentiality requirement does not apply to any disclosure to a Federal official for purposes of UC program oversight and audits, including disclosures under 20 CFR part 601 and 29 CFR parts 96 and 97.

[71 FR 56842, Sept. 27, 2006, as amended at 81 FR 56333, Aug. 19, 2016]

§603.6 What disclosures are required by this subpart?

- (a) The confidentiality requirement of 303(a)(1), SSA, and §603.4 are not applicable to this paragraph (a) and the Department of Labor interprets Section 303(a)(1), SSA, as requiring disclosure of all information necessary for the proper administration of the UC program. This includes disclosures to claimants, employers, the Internal Revenue Service (for purposes of UC tax administration), and the U.S. Citizenship and Immigration Services (for purposes of verifying a claimant’s immigration status).
- (b) In addition to Section 303(f), SSA (concerning an IEVS), which is addressed in subpart C, the following provisions of Federal UC law also specifically require disclosure of State UC information and State-held information pertaining to the Federal UC and benefit programs of Unemployment Compensation for Federal Employees (UCFE), Unemployment Compensation for Ex-Servicemembers (UCX), Trade Adjustment Assistance (TAA) (except for confidential business information collected by States), Disaster Unemployment Assistance (DUA), and any Federal UC benefit extension program:
 - (1) Section 303(a)(7), SSA, requires State law to provide for making available, upon request, to any agency of the United States charged with the administration of public works or assistance through public employment, disclosure of the following information with respect to each recipient of UC—
 - (i) Name;
 - (ii) Address;
 - (iii) Ordinary occupation;
 - (iv) Employment status; and
 - (v) A statement of such recipient’s rights to further compensation under the State law.
 - (2) Section 303(c)(1), SSA, requires each State to make its UC records available to the Railroad Retirement Board, and to furnish such copies of its UC records to the Railroad Retirement Board as the Board deems necessary for its purposes.
 - (3) Section 303(d)(1), SSA, requires each State UC agency, for purposes of determining an individual’s eligibility benefits, or the amount of benefits, under a food stamp program established under the Food Stamp Act of 1977, to disclose, upon request, to officers and employees of the Department of Agriculture, and to officers or employees of any State food stamp agency, any of the following information contained in the records of the State UC agency—

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

- (i) Wage information,
 - (ii) Whether an individual is receiving, has received, or has made application for, UC, and the amount of any such compensation being received, or to be received, by such individual,
 - (iii) The current (or most recent) home address of such individual, and
 - (iv) Whether an individual has refused an offer of employment and, if so, a description of the employment so offered and the terms, conditions, and rate of pay therefore.
- (4) Section 303(e)(1), SSA, requires each State UC agency to disclose, upon request, directly to officers or employees of any State or local child support enforcement agency, any wage information contained in the records of the State UC agency for purposes of establishing and collecting child support obligations (not to include custodial parent support obligations) from, and locating, individuals owing such obligations.
- (5) Section 303(h), SSA, requires each State UC agency to disclose quarterly, to the Secretary of Health and Human Services (HHS), wage information and claim information as required under Section 453(i)(1) of the SSA (establishing the National Directory of New Hires), contained in the records of such agency, for purposes of Subsections (i)(1), (i)(3), and (j) of Section 453, SSA (establishing the National Directory of New Hires and its uses for purposes of child support enforcement, Temporary Assistance to Needy Families (TANF), TANF research, administration of the earned income tax credit, and use by the Social Security Administration).
- (6) Section 303(i), SSA, requires each State UC agency to disclose, upon request, to officers or employees of the Department of Housing and Urban Development (HUD) and to representatives of a public housing agency, for purposes of determining an individual's eligibility for benefits, or the amount of benefits, under a housing assistance program of HUD, any of the following information contained in the records of such State agency about any individual applying for or participating in any housing assistance program administered by HUD who has signed a consent form approved by the Secretary of HUD—
 - (i) Wage information, and
 - (ii) Whether the individual is receiving, has received, or has made application for, UC, and the amount of any such compensation being received (or to be received) by such individual.
- (7) Section 3304(a)(16), FUTA requires each State UC agency—
 - (i) To disclose, upon request, to any State or political subdivision thereof administering a Temporary Assistance to Needy Families Agency (TANF) program funded under part A of Title IV of the SSA, wage information contained in the records of the State UC agency which is necessary (as determined by the Secretary of HHS in regulations) for purposes of determining an individual's eligibility for TANF assistance or the amount of TANF assistance; and
 - (ii) To furnish to the Secretary of HHS, in accordance with that Secretary's regulations at 45 CFR 303.108, wage information (as defined at 45 CFR 303.108(a)(2)) and UC information (as defined at 45 CFR 303.108(a)(3)) contained in the records of such agency for the purposes of the National Directory of New Hires established under Section 453(i) of the SSA.
- (8) To comply with WIOA sec. 116(e)(4), States must, to the extent practicable, cooperate in the conduct of evaluations (including related research projects) provided for by the Secretary of Labor or the Secretary of Education under the provisions of Federal law identified in WIOA sec. 116(e)(1); WIOA secs. 169 and 242(c)(2)(D); sec. 12(a)(5), 14, and 107 of the Rehabilitation Act of 1973 (29 U.S.C. 709(a)(5), 711, 727) (applied with respect to programs carried out under title I of that Act (29 U.S.C. 720 *et seq.*)); and the investigations provided for by the Secretary of Labor under sec. 10(b) of the Wagner-Peyser Act (29 U.S.C. 49i(b)). For purposes of this part, States must disclose confidential UC information to a Federal official (or an agent or contractor of a Federal official) requesting such information in the course of such evaluations. This disclosure must be done in accordance with appropriate privacy and confidentiality protections established in this part. This disclosure must be

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

made to the “extent practicable”, which means that the disclosure would not interfere with the efficient administration of the State UC law, as required by §603.5.

- (c) Each State law must contain provisions that are interpreted and applied consistently with the requirements listed in this section.

[71 FR 56842, Sept. 27, 2006, as amended at 81 FR 56333, Aug. 19, 2016]

§603.7 What requirements apply to subpoenas, other compulsory processes, and disclosure to officials with subpoena authority?

- (a) *In general.* Except as provided in paragraph (b) of this section, when a subpoena or other compulsory process is served upon a State UC agency or the State, any official or employee thereof, or any recipient of confidential UC information, which requires the production of confidential UC information or appearance for testimony upon any matter concerning such information, the State or State UC agency or recipient must file and diligently pursue a motion to quash the subpoena or other compulsory process if other means of avoiding the disclosure of confidential UC information are not successful or if the court has not already ruled on the disclosure. Only if such motion is denied by the court or other forum may the requested confidential UC information be disclosed, and only upon such terms as the court or forum may order, such as that the recipient protect the disclosed information and pay the State’s or State UC agency’s costs of disclosure.
- (b) *Exceptions.* The requirement of paragraph (a) of this section to move to quash subpoenas shall not be applicable, so that disclosure is permissible, where—
- (1) *Court Decision*—a subpoena or other compulsory legal process has been served and a court has previously issued a binding precedential decision that requires disclosures of this type, or a well-established pattern of prior court decisions have required disclosures of this type, or
 - (2) *Official with subpoena authority*—Confidential UC information has been subpoenaed, by a local, State or Federal governmental official, other than a clerk of court on behalf of a litigant, with authority to obtain such information by subpoena under State or Federal law. The State or State UC agency may choose to disclose such confidential UC information to these officials without the actual issuance of a subpoena.

§603.8 What are the requirements for payment of costs and program income?

- (a) *In general.* Except as provided in paragraph (b) of this section, grant funds must not be used to pay any of the costs of making any disclosure of UC information. Grant funds may not be used to pay any of the costs of making any disclosures under §603.5(d)(2) (third party (other than an agent) or disclosure made on an ongoing basis), §603.5(e) (optional disclosure to a public official), §603.5(f) (optional disclosure to an agent or contractor of a public official), and §603.5(g) (optional disclosure to BLS), §603.6(b) (mandatory disclosures for non-UC purposes), or §603.22 (mandatory disclosure for purposes of an IEVS).
- (b) *Use of grant funds permitted.* Grant funds paid to a State under Section 302(a), SSA, may be used to pay the costs of only those disclosures necessary for proper administration of the UC program. (This may include some disclosures under §603.5(a) (concerning public domain information), §603.5(c) (to an individual or employer), and §603.5(d)(1) (to an agent).) In addition, grant funds may be used to pay costs of disclosures under §603.5(i) (for UC Program Oversight and Audits) and §603.6(a) (for the proper administration of the UC program). Grant funds may also be used to pay costs associated with disclosures under §603.7(b)(1) (concerning court-ordered compliance with subpoenas) if a court has denied recovery of costs, or to pay costs associated with disclosures under §603.7(b)(2) (to officials with subpoena authority) if the State UC agency has attempted but not been successful in obtaining reimbursement of costs. Finally, grant funds may be used to pay costs associated with any disclosure of UC information if not more than an incidental amount of staff time and no more than nominal processing costs are involved in making the disclosure.
- (c) *Calculation of costs.* The costs to a State or State UC agency of processing and handling a request for disclosure of information must be calculated in accordance with the cost principles and administrative requirements of 29 CFR part 97 and Office of Management and Budget Circular No. A-87 (Revised). For

the purpose of calculating such costs, any initial start-up costs incurred by the State UC agency in preparation for making the requested disclosure(s), such as computer reprogramming necessary to respond to the request, and the costs of implementing safeguards and agreements required by §§603.9 and 603.10, must be charged to and paid by the recipient. (Start-up costs do not include the costs to the State UC agency of obtaining, compiling, or maintaining information for its own purposes.) Postage or other delivery costs incurred in making any disclosure are part of the costs of making the disclosure. Penalty mail, as defined in 39 U.S.C. 3201(1), must not be used to transmit information being disclosed, except information disclosed for purposes of administration of State UC law. As provided in Sections 453(e)(2) and 453(g) of the SSA, the Secretary of HHS has the authority to determine what constitutes a reasonable amount for the reimbursement for disclosures under Section 303(h), SSA, and Section 3304(a)(16)(B), FUTA.

- (d) *Payment of costs.* The costs to a State or State UC agency of making a disclosure of UC information, calculated in accordance with paragraph (c) of this section, must be paid by the recipient of the information or another source paying on behalf of the recipient, either in advance or by way of reimbursement. If the recipient is not a public official, such costs, except for good reason must be paid in advance. For the purposes of this paragraph (d), payment in advance means full payment of all costs before or at the time the disclosed information is given in hand or sent to the recipient. The requirement of payment of costs in this paragraph is met when a State UC agency has in place a reciprocal cost agreement or arrangement with the recipient. As used in this section, *reciprocal* means that the relative benefits received by each are approximately equal. Payment or reimbursement of costs must include any initial start-up costs associated with making the disclosure.
- (e) *Program income.* Costs paid as required by this section, and any funds generated by the disclosure of UC information under this part, are program income and may be used only as permitted by 29 CFR 97.25(g) (on program income). Such income may not be used to benefit a State's general fund or other program.

§603.9 What safeguards and security requirements apply to disclosed information?

- (a) *In general.* For disclosures of confidential UC information under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis); §603.5(e) (to a public official), except as provided in paragraph (d) of this section; §603.5(f) (to an agent or contractor of a public official); §603.6(b)(1) through (4), (6), and (7)(i) (as required by Federal UC law); and §603.22 (to a requesting agency for purposes of an IEVS), a State or State UC agency must require the recipient to safeguard the information disclosed against unauthorized access or redisclosure, as provided in paragraphs (b) and (c) of this section, and must subject the recipient to penalties provided by the State law for unauthorized disclosure of confidential UC information.
- (b) *Safeguards to be required of recipients.*
 - (1) The State or State UC agency must:
 - (i) Require the recipient to use the disclosed information only for purposes authorized by law and consistent with an agreement that meets the requirements of §603.10;
 - (ii) Require the recipient to store the disclosed information in a place physically secure from access by unauthorized persons;
 - (iii) Require the recipient to store and process disclosed information maintained in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot obtain the information by any means;
 - (iv) Require the recipient to undertake precautions to ensure that only authorized personnel are given access to disclosed information stored in computer systems;
 - (v) Require each recipient agency or entity to:
 - (A) Instruct all personnel having access to the disclosed information about confidentiality requirements, the requirements of this subpart B, and the sanctions specified in the State law for unauthorized disclosure of information, and

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

- (B) Sign an acknowledgment that all personnel having access to the disclosed information have been instructed in accordance with paragraph (b)(1)(v)(A) of this section and will adhere to the State's or State UC agency's confidentiality requirements and procedures which are consistent with this subpart B and the agreement required by §603.10, and agreeing to report any infraction of these rules to the State UC agency fully and promptly,
 - (vi) Require the recipient to dispose of information disclosed or obtained, and any copies thereof made by the recipient agency, entity, or contractor, after the purpose for which the information is disclosed is served, except for disclosed information possessed by any court. Disposal means return of the information to the disclosing State or State UC agency or destruction of the information, as directed by the State or State UC agency. Disposal includes deletion of personal identifiers by the State or State UC agency in lieu of destruction. In any case, the information disclosed must not be retained with personal identifiers for longer than such period of time as the State or State UC agency deems appropriate on a case-by-case basis; and
 - (vii) Maintain a system sufficient to allow an audit of compliance with the requirements of this part.
- (2) In the case of disclosures made under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis), the State or State UC agency must also—
- (i) Periodically audit a sample of transactions accessing information disclosed under that section to assure that the entity receiving disclosed information has on file a written release authorizing each access. The audit must ensure that the information is not being used for any unauthorized purpose;
 - (ii) Ensure that all employees of entities receiving access to information disclosed under §603.5(d)(2) are subject to the same confidentiality requirements, and State criminal penalties for violation of those requirements, as are employees of the State UC agency.
- (c) *Redisclosure of confidential UC information.*
- (1) A State or State UC agency may authorize any recipient of confidential UC information under paragraph (a) of this section to redisclose information only as follows:
- (i) To the individual or employer who is the subject of the information;
 - (ii) To an attorney or other duly authorized agent representing the individual or employer;
 - (iii) In any civil or criminal proceedings for or on behalf of a recipient agency or entity;
 - (iv) In response to a subpoena only as provided in §603.7;
 - (v) To an agent or contractor of a public official only if the person redisclosing is a public official, if the redisclosure is authorized by the State law, and if the public official retains responsibility for the uses of the confidential UC information by the agent or contractor;
 - (vi) From one public official to another if the redisclosure is authorized by the State law;
 - (vii) When so authorized by Section 303(e)(5), SSA, (redisclosure of wage information by a State or local child support enforcement agency to an agent under contract with such agency for purposes of carrying out child support enforcement) and by State law; or
 - (viii) When specifically authorized by a written release that meets the requirements of §603.5(d) (to a third party with informed consent).
- (2) Information redisclosed under paragraphs (c)(1)(v) and (vi) of this section must be subject to the safeguards in paragraph (b) of this section.
- (d) The requirements of this section do not apply to disclosures of UC information to a Federal agency which the Department has determined, by notice published in the *FEDERAL REGISTER*, to have in place safeguards adequate to satisfy the confidentiality requirement of Section 303(a)(1), SSA.

§603.10 What are the requirements for agreements?

(a) Requirements.

- (1) For disclosures of confidential UC information under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis); §603.5(e) (to a public official), except as provided in paragraph (d) of this section; §603.5(f) (to an agent or contractor of a public official); §603.6(b)(1)

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

through (4), (6), and (7)(i) (as required by Federal UC law); and §603.22 (to a requesting agency for purposes of an IEVS), a State or State UC agency must enter into a written, enforceable agreement with any agency or entity requesting disclosure(s) of such information. The agreement must be terminable if the State or State UC agency determines that the safeguards in the agreement are not adhered to.

- (2) For disclosures referred to in §603.5(f) (to an agent or contractor of a public official), the State or State UC agency must enter into a written, enforceable agreement with the public official on whose behalf the agent or contractor will obtain information. The agreement must hold the public official responsible for ensuring that the agent or contractor complies with the safeguards of §603.9. The agreement must be terminable if the State or State UC agency determines that the safeguards in the agreement are not adhered to.

(b) *Contents of agreement—*

- (1) *In general.* Any agreement required by paragraph (a) of this section must include, but need not be limited to, the following terms and conditions:
- (i) A description of the specific information to be furnished and the purposes for which the information is sought;
 - (ii) A statement that those who request or receive information under the agreement will be limited to those with a need to access it for purposes listed in the agreement;
 - (iii) The methods and timing of requests for information and responses to those requests, including the format to be used;
 - (iv) Provision for paying the State or State UC agency for any costs of furnishing information, as required by §603.8 (on costs);
 - (v) Provision for safeguarding the information disclosed, as required by §603.9 (on safeguards); and
 - (vi) Provision for on-site inspections of the agency, entity, or contractor, to assure that the requirements of the State's law and the agreement or contract required by this section are being met.
- (2) In the case of disclosures under §603.5(d)(2) (to a third party (other than an agent) or disclosures made on an ongoing basis), the agreement required by paragraph (a) of this section must assure that the information will be accessed by only those entities with authorization under the individual's or employer's release, and that it may be used only for the specific purposes authorized in that release.

(c) *Breach of agreement—*

- (1) *In general.* If an agency, entity, or contractor, or any official, employee, or agent thereof, fails to comply with any provision of an agreement required by this section, including timely payment of the State's or State UC agency's costs billed to the agency, entity, or contractor, the agreement must be suspended, and further disclosure of information (including any disclosure being processed) to such agency, entity, or contractor is prohibited, until the State or State UC agency is satisfied that corrective action has been taken and there will be no further breach. In the absence of prompt and satisfactory corrective action, the agreement must be canceled, and the agency, entity, or contractor must be required to surrender to the State or State UC agency all confidential UC information (and copies thereof) obtained under the agreement which has not previously been returned to the State or State UC agency, and any other information relevant to the agreement.
- (2) *Enforcement.* In addition to the actions required to be taken by paragraph (c)(1) of this section, the State or State UC agency must undertake any other action under the agreement, or under any law of the State or of the United States, to enforce the agreement and secure satisfactory corrective action or surrender of the information, and must take other remedial actions permitted under State or Federal law to effect adherence to the requirements of this subpart B, including seeking damages, penalties, and restitution as permitted under such law for any charges to granted funds and all costs incurred by the State or the State UC agency in pursuing the breach of the agreement and enforcement as required by this paragraph (c).

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

- (d) The requirements of this section do not apply to disclosures of UC information to a Federal agency which the Department has determined, by notice published in the *FEDERAL REGISTER*, to have in place safeguards adequate to satisfy the confidentiality requirement of Section 303(a)(1), SSA, and an appropriate method of paying or reimbursing the State UC agency (which may involve a reciprocal cost arrangement) for costs involved in such disclosures. These determinations will be published in the *FEDERAL REGISTER*.

§603.11 How do States notify claimants and employers about the uses of their information?

- (a) *Claimants.* Every claimant for compensation must be notified, at the time of application, and periodically thereafter, that confidential UC information pertaining to the claimant may be requested and utilized for other governmental purposes, including, but not limited to, verification of eligibility under other government programs. Notice on or attached to subsequent additional claims will satisfy the requirement for periodic notice thereafter.
- (b) *Employers.* Every employer subject to a State's law must be notified that wage information and other confidential UC information may be requested and utilized for other governmental purposes, including, but not limited to, verification of an individual's eligibility for other government programs.

§603.12 How are the requirements of this part enforced?

- (a) *Resolving conformity and compliance issues.* For the purposes of resolving issues of conformity and substantial compliance with the requirements set forth in subparts B and C, the provisions of 20 CFR 601.5(b) (informal discussions with the Department of Labor to resolve conformity and substantial compliance issues), and 20 CFR 601.5(d) (Secretary of Labor's hearing and decision on conformity and substantial compliance) apply.
- (b) *Conformity and substantial compliance.* Whenever the Secretary of Labor, after reasonable notice and opportunity for a hearing to the State UC agency of a State, finds that the State law fails to conform, or that the State or State UC agency fails to comply substantially, with:
- (1) The requirements of Title III, SSA, implemented in subparts B and C of this part, the Secretary of Labor shall notify the Governor of the State and such State UC agency that further payments for the administration of the State UC law will not be made to the State until the Secretary of Labor is satisfied that there is no longer any such failure. Until the Secretary of Labor is so satisfied, the Department of Labor shall make no further payments to such State.
 - (2) The FUTA requirements implemented in this subpart B, the Secretary of Labor shall make no certification under that section to the Secretary of the Treasury for such State as of October 31 of the 12-month period for which such finding is made.

Subpart C—Mandatory Disclosure for Income and Eligibility Verification System (IEVS)

§603.20 What is the purpose and scope of this subpart?

- (a) *Purpose.* Subpart C implements Section 303(f), SSA. Section 303(f) requires States to have in effect an income and eligibility verification system, which meets the requirements of Section 1137, SSA, under which information is requested and exchanged for the purpose of verifying eligibility for, and the amount of, benefits available under several federally assisted programs, including the Federal-State UC program.

- (b) *Scope.* This subpart C applies only to a State UC agency.

NOTE TO PARAGRAPH (b): Although not implemented in this part 603, Section 1137(a)(1), SSA, provides that each State must require claimants for compensation to furnish to the State UC agency their social security account numbers, as a condition of eligibility for compensation, and further requires States to utilize such account numbers in the administration of the State UC laws. Section 1137(a)(3), SSA, further provides that employers must make quarterly wage reports to a State UC agency, or an alternative agency, for use in verifying eligibility for, and the amount of, benefits. Section 1137(d)(1), SSA, provides that each State must require claimants for compensation, as a condition of eligibility, to declare in writing, under penalty of perjury, whether the individual is a citizen or national of the United States, and, if not, that the individual is in a satisfactory immigration status. Other provisions of Section 1137(d), SSA, not implemented in

ATTACHMENT 3—UC Confidentiality and Disclosure Regulations—20 CFR Part 603

this regulation require the States to obtain, and individuals to furnish, information which shows immigration status, and require the States to verify immigration status with the Bureau of Citizenship and Immigration Services.

§603.21 What is a requesting agency?

For the purposes of this subpart C, *requesting agency* means:

- (a) *Temporary Assistance to Needy Families Agency*—Any State or local agency charged with the responsibility of administering a program funded under part A of Title IV of the SSA.
- (b) *Medicaid Agency*—Any State or local agency charged with the responsibility of administering the provisions of the Medicaid program under a State plan approved under Title XIX of the SSA.
- (c) *Food Stamp Agency*—Any State or local agency charged with the responsibility of administering the provisions of the Food Stamp Program under the Food Stamp Act of 1977.
- (d) *Other SSA Programs Agency*—Any State or local agency charged with the responsibility of administering a program under a State plan approved under Title I, X, XIV, or XVI (Supplemental Security Income for the Aged, Blind, and Disabled) of the SSA.
- (e) *Child Support Enforcement Agency*—Any State or local child support enforcement agency charged with the responsibility of enforcing child support obligations under a plan approved under part D of Title IV of the SSA.
- (f) *Social Security Administration*—Commissioner of the Social Security Administration in establishing or verifying eligibility or benefit amounts under Titles II (Old-Age, Survivors, and Disability Insurance Benefits) and XVI (Supplemental Security Income for the Aged, Blind, and Disabled) of the SSA.

§603.22 What information must State UC agencies disclose for purposes of an IEVS?

- (a) *Disclosure of information.* Each State UC agency must disclose, upon request, to any requesting agency, as defined in §603.21, that has entered into an agreement required by §603.10, wage information (as defined at §603.2(k)) and claim information (as defined at §603.2(a)) contained in the records of such State UC agency.
- (b) *Format.* The State UC agency must adhere to standardized formats established by the Secretary of HHS (in consultation with the Secretary of Agriculture) and set forth in 42 CFR 435.960 (concerning standardized formats for furnishing and obtaining information to verify income and eligibility).

§603.23 What information must State UC agencies obtain from other agencies, and crossmatch with wage information, for purposes of an IEVS?

- (a) *Crossmatch with information from requesting agencies.* Each State UC agency must obtain such information from the Social Security Administration and any requesting agency as may be needed in verifying eligibility for, and the amount of, compensation payable under the State UC law.
- (b) *Crossmatch of wage and benefit information.* The State UC agency must crossmatch quarterly wage information with UC payment information to the extent that such information is likely, as determined by the Secretary of Labor, to be productive in identifying ineligibility for benefits and preventing or discovering incorrect payments.

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION Personally Identifiable Information
	CORRESPONDENCE SYMBOL OFAM
	DATE June 28, 2012

ADVISORY: TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 39-11

TO: ALL DIRECT ETA GRANT RECIPIENTS
 ALL STATE WORKFORCE AGENCIES
 ALL STATE WORKFORCE LIAISONS
 STATE WORKFORCE ADMINISTRATORS
 STATE AND LOCAL WORKFORCE INVESTMENT BOARDS
 ONE-STOP CAREER CENTER SYSTEM LEADS

FROM: JANE OATES /s/
 Assistant Secretary

SUBJECT: Guidance on the Handling and Protection of Personally Identifiable Information (PII)

1. Purpose. To provide guidance to grantees on compliance with the requirements of handling and protecting PII in their grants.

2. Background. As part of their grant activities, Employment and Training Administration (ETA) grantees may have in their possession large quantities of PII relating to their organization and staff; subgrantee and partner organizations and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources.

Federal agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. The Appendix lists a brief overview of efforts at the Federal level to protect PII. As the grantor agency, ETA is providing this Training and Employment Guidance Letter (TEGL) to grantees to notify them of the specific requirements grantees must follow pertaining to the acquisition, handling, and transmission of PII.

3. Definitions.

- PII - OMB defines PII as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.¹

¹OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at <http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf>

RESCISSIONS None	EXPIRATION DATE Continuing
----------------------------	--------------------------------------

- Sensitive Information – any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.
- Protected PII and non-sensitive PII - the Department of Labor (the Department) has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the “risk of harm” that could result from the release of the PII.
 1. Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.
 2. Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and mother’s maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

4. Requirements. Federal law, OMB Guidance, and Departmental and ETA policies require that PII and other sensitive information be protected. ETA has examined the ways its grantees, as stewards of Federal funds, handle PII and sensitive information and has determined that to ensure ETA compliance with Federal law and regulations, grantees must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.

In addition to the requirement above, all grantees must also comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated

cryptographic module.² Grantees must not e-mail unencrypted sensitive PII to any entity, including ETA or contractors.

- Grantees must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. Grantees must maintain such PII in accordance with the ETA standards for information security described in this TEGL and any updates to such standards provided to the grantee by ETA. Grantees who wish to obtain more information on data security should contact their Federal Project Officer.
- Grantees shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.
- Grantees further acknowledge that all PII data obtained through their ETA grant shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using grantee issued equipment, managed information technology (IT) services, and designated locations approved by ETA. Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-grantee managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by ETA.
- Grantee employees and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.
- Grantees must have their policies and procedures in place under which grantee employees and other personnel, before being granted access to PII, acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.
- Grantees must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.
- Access to any PII created by the ETA grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

²For more information on FIPS 140-2 standards and cryptographic modules, grantees should refer to FIPS PUB 140-2, located online at: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

- All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.
- PII data obtained by the grantee through a request from ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer.
- Grantees must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, grantees must make records applicable to this Agreement available to authorized persons for the purpose of inspection, review, and/or audit.
- Grantees must retain data received from ETA only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

A grantee's failure to comply with the requirements identified in this TEG, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant, or the imposition of special conditions or restrictions, or such other actions as the Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

5. Recommendations. Protected PII is the most sensitive information that you may encounter in the course of your grant work, and it is important that it stays protected. Grantees are required to protect PII when transmitting information, but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well. Outlined below are some recommendations to help protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.
- Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to the each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended.
- Store documents containing PII in locked cabinets when not in use.
- Immediately report any breach or suspected breach of PII to the FPO responsible for the grant, and to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

6. Inquiries. Questions should be addressed to the appropriate Regional Office.

7. Attachment. Appendix: *Applicable Federal Laws and Policies Related To Data Privacy, Security and Protecting Personally Identifiable and Sensitive Information*

APPENDIX

FEDERAL LAWS AND POLICIES RELATED TO DATA PRIVACY, SECURITY AND PROTECTING PERSONALLY IDENTIFIABLE AND SENSITIVE INFORMATION

- Privacy Act of 1974 (the Privacy Act) – Governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by Federal agencies. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the individual, unless the disclosure is permissible under one of twelve statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amendment of their records and establishes various agency record-keeping requirements. The Privacy Act does not generally apply to personally identifiable information collected and maintained by grantees.
- Computer Security Act of 1987 – Passed to improve the security and privacy of sensitive information in Federal computer systems and created a means for establishing minimum acceptable security practices for such systems. It required agencies to identify their computer systems that contained sensitive information, create computer security plans, and provide security training of system users or owners on the systems that house sensitive information. It was repealed by the Federal Information Security Management Act (FISMA).
- FISMA – Enacted as Title III of the E-Government Act of 2002, FISMA required each Federal agency to develop and implement an agency-wide program to safeguard the information and information systems that support the operational assets of the agency, including the assets managed by other agencies or contractors.
- On May 22, 2006, the Office of Management and Budget (OMB) issued M-06-15, *Safeguarding Personally Identifiable Information*. In this memorandum, OMB directed Senior Officials for Privacy to conduct a review of agency policies and processes and to take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to, PII.
- On July 12, 2006, OMB issued M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. In this memorandum, OMB provided updated guidance for reporting of security incidents involving PII.
- On May 10, 2006, Executive Order 13402 established the President’s Task Force on Identity Theft. The Task Force was charged with developing a comprehensive strategic plan for steps the Federal government can take to combat identity theft and recommending actions which can be taken by the public and private sectors. On April 23, 2007, the Task Force submitted its report to the President, titled “Combating Identity Theft: A Strategic Plan.” This report is available at www.idtheft.gov.

- On May 22, 2007, OMB issued M 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. In this memorandum, OMB required agencies to implement a PII breach notification policy within 120 days.
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII – Released by NIST in April 2010, this document is a guide to assist Federal agencies in protecting the confidentiality of PII in information systems. The guide explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.